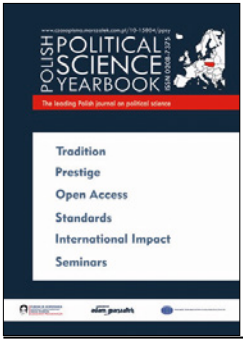

Polish Political Science Yearbook

ISSN: 0208–7375 Journal homepage: https://czasopisma.marszalek.com.pl/10-15804/ppsy

Cybercrime on the Example of Selected Botnets

Przemysław Mazurczak
ORCID: 0000-0003-2986-8607

To cite this article please include the following information:
- Journal title: Polish Political Science Yearbook
- Volume number: 50
- Year of publication: 2021
- Published ahead-of-print

Example styles:

[APA Style]: Mazurczak, P. (2021). Cybercrime on the Example of Selected Botnets. *Polish Political Science Yearbook, 50*(issue number), pages. https://doi.org/10.15804/ppsy202138

[Chicago Style]: Przemysław Mazurczak, "Cybercrime on the Example of Selected Botnets" *Polish Political Science Yearbook* 50, no. [issue number] (2021).

To link to this article: https://doi.org/10.15804/ppsy202138

Published ahead-of-print

Final submission:	6 July 2021
Published online:	16 July 2021
Printed issue:	2021

Polish Political Science Yearbook, **vol. 50 (2021), pp. 1–13**
DOI: https://doi.org/10.15804/ppsy202138 PL ISSN 0208-7375
www.czasopisma.marszalek.com.pl/10-15804/ppsy

Przemysław Mazurczak
Siedlce University of Natural Sciences and Humanities (Poland)
ORCID: 0000-0003-2986-8607
e-mail: mazurczak.przemek@vp.pl

Cybercrime on the Example of Selected Botnets

Abstract: The article presents threat analysis resulting from botnet activity on the Internet. Botnet networks are a very common tool among cybercriminals. They enable the acquisition of large amounts of data from computers infected with the virus that creates the given network entirely subordinated to its creator. Currently, many unidentified botnets are a threat to Internet users. Those identified and diagnosed answer the problem of how dangerous a botnet is in the hands of cybercriminals. The article presents statistics and analysis of selected botnets. Currently, there is a decline in the interest in botnets in cybercrime, although many new threats appear, suggesting that botnets will continue to be popular and are still a dangerous weapon in the hands of criminals.

Keywords: *cyber threats, botnet, computer network, cyberspace, cybersecurity*

Introduction

The challenges related to cyber threats are now the core content of most countries and international organizations' preparatory and operational security strategies (Grzelak & Liedel, 2012). The developed strategies emphasize the need to pay special attention to the new space in which modern societies function – the so-called cyberspace. Research is conducted in many research centers and in the armies of most countries of the world to develop methods and specialized tools to increase the effectiveness of detecting, counteracting, and neutralizing the effects of cyber threats. The need to develop such methods and tools results from the increasing dependence of the state administration, private institutions, and the entire society on communication networks and IT systems (Antkiewicz et al., 2014, pp. 93-102).

In Poland, despite the ever-increasing number of publications, knowledge about the latest trends in threats from networks and computer systems is a kind of specialist knowledge inaccessible and often incomprehensible to a large part of the society (Siwicki, 2013, p. 7). Lack of up-to-date knowledge of the latest trends is a threat to Internet users. It contributes

to disregarding the security measures, hacking into computer systems without being noticed, the low willingness of crime victims to get the police involved in prosecutions, and the low probability of detecting the persecutor. Consequently, the organized crime makes huge financial profits with minimal risk of accountability for criminal liability. Counteracting such a crime is exceedingly difficult and expensive. It requires financial, organizational, or technical investment and increased awareness of network users and law enforcement authorities about the threats caused by cybercrime.

The purpose of this article is to characterize cybercrime based on botnet tools used by criminals around the world. The article was written based on compact sources, journals, and scientific articles. The considerations contained in it may be a source of knowledge about the activities of cybercriminals and the functioning of botnets, including tips on how to protect themselves against unwanted activities on their part. The knowledge available in the article has been enriched with the author's experiences and thoughts, which bring new knowledge to the area described.

1. Historical Overview

The development of cybercrime was simultaneous with the growth of information society. During the early 1960s in the US, when computers were first introduced, criminals thought about the ways and the possibilities of implementing new technologies and using them for criminal purposes. The constant technological progress provided cybercriminals with new tools. The advent of cryptocurrencies revolutionized the cash changeover and allowed for anonymous payments, which sparked a particular interest in crime.

The history of botnets dates back to the late 1980s, when the Morris Worm was created, capable of automatically infecting other systems connected to the Internet. It infected 6,000 computers, which was then one-fifth of all computers connected to the Internet in the world. Its creator Robert Morris was tried and convicted. The first botnets could already conduct real-time conversations on communication channels and control malware using transmitted messages (Maj, 2015). Cybercriminals created the Storm botnet in 2007. It was such an advanced network that it could disconnect entire countries from the Internet, as confirmed by security experts. The network consisted of about 2 million infected machines and had computing power exceeding that of supercomputers at the time. However, the most powerful botnet in history was created in 2009, called BredoLab. Malware affected more than 30 million computers, providing networks with unimaginable possibilities. The botnet was partially neutralized only at the end of 2010. In the first decade of the 21st century, the cryptocurrency market was relatively poor. It is worth paying attention if any of these large botnets could be used to mine cryptocurrencies. The use of such powerful computing power could bring a botnet owner a high income. Currently, botnet-related technologies are constantly expanded and improved so that new viruses can circumvent the latest security measures and give the best possible results, contributing to the development of cybercrime (Czym jest Botnet?, 2015).

The main reason for the development of cybercrime is the possibility of achieving very high profits with relatively low risk and low financial outlay. Criminals look for money where there is most money, so part of the cybercrime concerns the banking sector. Stealing money from a bank is a dream of many criminals. However, nowadays, traditional armed robberies are rare. There is an extremely high risk of failure and apprehension of perpetrators by police. In the case of remote attacks, the situation is entirely different. The criminal has a much greater chance of success with minimalist chances of being caught. Considering such a scenario, criminals have created one of the most effective tools for robbing a bank – Botnet with the mythical-sounding name ZEUS.

2. Characteristics of Botnet

A botnet is a group of computers infected with malicious software, e.g., a computer worm or a Trojan hidden from the user and allowing its creator to exercise remote control over all computers created within the network (Hołyst & Pomykała, 2012, p. 14). These networks are the most common and often perceived as extremely important from the point of view of state security (Kasprzyk et al., 2015, p. 83). Devices included in the botnet are called bots. In order to exist, they must be consisted of at least two devices infected with malware. The aim of the Botnet creators is to infect as many computers and devices connected with the Internet as possible. Botnets can be composed of several million bots. The known ones include, for example, Mirai, Conficker, Zeus, Waledac, Mariposa, and Kelihos.

The specificity of botnets operation is based on the use of computing power of interconnected computers. Botnets are created by viruses and computer worms, i.e., self-replicating viruses programs that do not need an executable file for infection, unlike the classic virus. In this respect, the computer worm is self-contained and can spread on the network by exploiting gaps in the operating system or the naivety of the user. Viruses or computer worms spread through various communication channels, most often through e-mail spam, instant messaging clients, and impersonating software available for download on the Internet.

Botnets are nowadays a big threat. The integration of even several computers connected to the Internet can be a useful tool for cybercriminals. There is no specific data on the number of botnets in the world. Botnets can be used for various attacks, including DDoS, data theft, robbery, sabotage, or surveillance.

Botnets are multi-tasking and can be used for many activities simultaneously. Cybercriminals most often use botnets for spamming, unwanted correspondence containing links or attachments with malware or advertising content. It is estimated that up to 80% of spam on the Internet is sent by "zombie" computers, which are part of someone else's botnet. The addresses used to send spam to go to the "blacklists" of postal operators often go to the "spam" tab or are completely blocked. Notwithstanding, cybercriminals have already found a way around postal operator blockades. A computer infected with the virus, belonging to a relevant botnet, can send out spam using available communicators, including the owner's

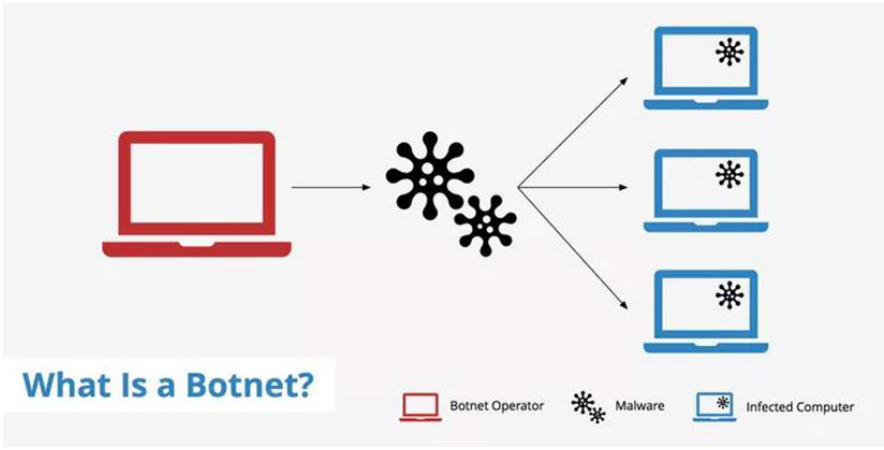

Figure 1. How the botnet works
Source: Keycdn, 2018.

mail, chat rooms, etc. It makes spam much more effective and dangerous. Spam sent from a trusted e-mail address or communicator is received as a "trusted source", e.g., through a network of friends on Facebook.

Distributed Denial of Service, i.e., blocking access to services on the Internet by generating artificial online traffic. This type is a very simple and reliable attack. It is based on the depletion of available server memory by overflowing and overloading, and suspending a given service or services. Cybercriminals use Botnet-linked zombie computers and access the server. As a result of overload, the server is blocked. Cybercriminals often demand a ransom to stop the attack, and companies often accept it, which is a faster solution than the action of law enforcement authorities. Hypothetically, a cybercriminal having a botnet of about 100 thousand bots can suspend for some time streaming services whose architecture hinders making an effective DDoS attack (Masywny 13-dniowy atak…, n.d.).

Theft of private and valuable data. A computer infected with a virus inside a botnet is an interesting source of private data for cybercriminals. Cybercriminals are particularly interested in credit card numbers, private photos, correspondence, logins, and passwords for various services, e.g., to the banks. All data collected is used in different ways; private photos and correspondence may be used for blackmail, credit cards for theft, and logins, passwords together with personal data may be sold.

Generate false clicks on online advertising. Some advertising agencies pay for the display of advertisements. Payment is carried out via the Pay-Per-Click system. A proper large botnet using zombie computers can generate several thousand unique clicks from several thousand different computers in one day. Thanks to this, the botnet owner can make high

profits from the ads his bots click on. Botnet acts as a parasite using the operating capabilities of interconnected computers. Since the creation of Bitcoin and cryptocurrencies, there are "diggers" botnets that use their abilities to obtain virtual currency.

Botnets are most often classified by their architecture and network protocols used to communicate between infected computers. With regard to architecture, centralized and decentralized botnets are distinguished (Kasprzyk et al., 2015, p. 3). In the centralized model, the infected computers are connected to server management called C&C (Command and Control). After connecting with C&C, each infected computer is registered in a database, which stores, among other things, data concerning IP addresses and the location of botnet computers. The botnet owner has direct control by issuing commands in the control panel. This type of botnets are easy to use, but they are relatively easy to neutralize because they are connected to a specific, usually single C&C server. It is enough to take over or neutralize the server to remove the whole threat.

In the decentralized model – P2P (Peer-to-Peer) situation is more complicated because the botnet has a dispersed structure. It means that any infected computer with the virus can act as a management server. The architecture of this botnet allows criminals to access the botnet's network through individual computers. Every bot has a list of "contiguous" machines, and with the help of a single bot server, the botnet administrator can issue commands for the entire network without distinguishing the role of the C&C server. In practice, creating decentralized botnets is quite difficult. Each newly infected computer should be provided with a list of "contiguous" bots to which the botnet will be connected. Notwithstanding, combating decentralized botnets is much more complicated than combating centralized networks (Masywny 13-dniowy atak…, n.d.). The elimination of a single computer leads to cutting off only some bots from the network.

Mixed model botnets are sometimes created. Such structure makes it easier for cybercriminals to transmit the list of "neighbors" to newly infected computers that communicate with a central server from which they receive bot lists and then switch to P2P communication.

3. The Most Popular Botnet

The first botnet I would like to highlight is the mythical Zeus. Zeus is a computer virus that modifies the appearance of websites in order to obtain money by fraud. The program creates Botnet – a network of infected computers managed remotely by cybercriminals. Zeus is one of the largest botnets currently operating on the Internet. It is also known as Zbot, PRG, Wsnpoem, Gorhax, Kneber (Zeus Report, 2011). Zeus bots are Trojan horses whose main tasks are to steal bank account data using built-in key loggers that intercept buttons pressed on the keyboard. Zeus is a multifunctional tool for conducting acts against banking sector users. In addition to data theft, the virus allows to generate phishing campaigns and create fake websites that are illusively similar to the original ones. The amount of Zeus botnets is estimated at several million infected computers, 3.6 million of which are in the US. The

botnet's victims included Bank of America, NASA, Monster, ABC, Oracle, Cisco, Amazon, and BusinessWeek. By October 29, 2009, botnet sent more than 1.5 million phishing messages to Facebook. Botnet sent about 9 million fake messages impersonating Verizon Wireless between November 14-15, 2009.

Zeus is a program that only attacks computers and devices working in the Windows system. Infection of a computer with the ZEUS virus is often caused by accidental downloading of a dropper, i.e., a program that contains an injected attachment to download malware. The drive-by-download method is used for this. The method consists of a malicious script, which contains a link to the site hosting malware injected into the code of a site located on the server. After entering a similarly modified website, the user is redirected invisibly to the malicious address. The exploit (i.e., a program using errors in the software structure) is launched, and the malware is downloaded and installed on the victim's computer (Kaspersky Lab Polska, 2011).

After downloading, the Trojan horse is launched on the victim's computer. The virus is encrypted with cryptographic algorithms and updated remotely, so it is difficult for antivirus programs to detect it. Everything is hidden from the user. Zeus is injected into the two important system processes, depending on the software version, previously into winlogin.exe, responsible for the login function, and explorer.exe, responsible for displaying the Windows interface. Both processes are necessary during working in a Windows environment. The code injected into the process retrieves a configuration file from an external server containing a list of attacked banks, sites, used attack vectors, etc. When information from the configuration file is loaded, Zeus intercepts user-critical information (mainly login information) and periodically sends it to the external server.

The greatest number of attacks with the Zeus botnet took place in 2009-2012. Then Electronic Banking was gradually developing in Poland. The virus changed the appearance of the original page of the victim's bank to a doctored one, forcing the user to log in to the transactional service. The virus also sent a fake text message to the victim for potential payment authorization. In fact, it was an attempt to activate transfers without authorization using the so-called "trusted device". In Poland, the victims included users of two banks – ING Bank Śląski and mBank.

According to a Cert's report, the amount of Zeus botnets is estimated at several million infected computers, 3.6 million of which are in the US (Kaspersky Lab Polska, 2011). The botnet's victims included Bank of America, NASA, Monster, ABC, Oracle, Cisco, Amazon, and BusinessWeek. By October 29, 2009, botnet sent more than 1.5 million phishing messages to Facebook. Botnet sent about 9 million fake messages impersonating Verizon Wireless between November 14-15, 2009 (Analiza bota Zeus, 2011). On June 14, 2010, Trustee released a report on credit cards of fifteen banks from the US. On October 1, 2010, the FBI reported the existence of an international group of cybercriminals responsible for hacking into American computers and stealing approximately $70 million. In the US, 90 people were arrested; and in the UK and Ukraine (Zeus Report, 2011).

Zeus botnet also hit Polish Internet users. Polish Cert has been monitoring its activity since January 2009. The largest number of attacks in 2009-2010 were targeted at the banking sector and two Polish banks – PKO BP and ING Bank Śląski. Both banks were found in over two hundred configuration files of the virus (CP Report, 2010). The Cert team recorded use cases or modified versions of the virus every year. For instance, in 2012, 246 564 unique IP addresses were registered from which online traffic was generated by Zeus bots (CP Report, 2012). In 2013, after many publications of Zeus codes, the number of Polish IPs generated by the virus decreased to 12 193 (CP Report, 2013). A year later, this trend was maintained at a similar level of 12 513 (CP Report, 2014). In 2015, further decreases in virus activity could be observed, then the activity of the botnet accounted for only 3.60% of all botnets on the Polish Internet. The amount of Zeus in 2015 was set at 5 305 generated Ips (CP Report, 2015). A year later, the activity of the Trojan was scant; only 6 cases were observed (CP Report, 2016). In the following years, no more significant activity was reported, the virus was uncovered and known all over the world, so it was no longer a threat.

Although ZEUS in cybercrime is already an outdated virus, its new and improved versions have been released. In 2012, a new version of the virus appeared: Citadel and Zeus-P2P, which modified popular web browsers. A year later, when mobile technology became more common, cybercriminals created a special version of the virus, which attacked systems in smartphones. The software worked in systems based on Android and encouraged to update banking applications. Downloading an application developed by cybercriminals allowed access to the smartphone, who usually took over the authorization passwords of SMS and eventually stole all the funds available on the account.

A few years later, in 2016, the Polish Bank Association announced on its official website the appearance of further threats of the banking virus. Banks warned against a new version of Zeus called ZITMO, which urged users of e-banking services to install malware on PCs, tablets, and smartphones, especially with the Android operating system, used in e-banking services (Uwaga!..., 2016). Traditionally, the virus was aimed at stealing passwords, text messages, and authorization sessions, enabling transfer operations in electronic banking services and mobile applications. Currently, the structure of the Zeus virus is very well-known, yet there is no shortage of new solutions for attacks on e-banking users. Many programs use Zeus mechanisms and social engineering for phishing attempts (fraudulently obtaining data). The latest solutions can even be based on the base system architecture, such as the affair with Huawei in 2019 concerning the potential spying of Americans by China.

The second interesting example of a botnet that evolved during the heyday of mobile technology is Android.ZBot. It is a Trojan horse designed to steal money from bank accounts and posed a severe threat to users of the very popular Android system. The virus could steal logins and passwords of other confidential data by displaying false authorization forms on the work screens of various applications. Cybercriminals generated the appearance of these forms. The virus was hidden under the famous "Google Play Store" application, so it did not attract the attention of average users. The pivotal moment for the virus was the request for

administrator rights. The granting of the authorization resulted in taking control of the device. In this way, cybercriminals stole credit card numbers together with secret CVV codes and authorized transfers from the victim's bank applications.

Virus infection most often occurred by downloading uncertified applications from sources other than Google, e.g., pirate games or programs with full Android licenses. When a newly infected device is registered on the server, the Trojan received a command to check the user's bank account. If it detected the availability of funds, it automatically transferred a certain amount of money to the cybercriminals' bank accounts. Thus, AndroidZBot could access the bank accounts of users of Android devices and steal money in secret, using special SMS commands required by online banking services. What is more, the victim was not even aware of the theft because the Trojan intercepted all incoming messages from banks containing transaction verification codes (Trojan bankowy Android.ZBot…, 2015). Although the virus was a typical "bank botnet", it also had the unique function of stealing various confidential data. It was done by using false input forms generated from commands received from the server and designed to create the illusion that they belong to some programs. Even though it was a classic phishing attack, the way it was conducted is quite exceptional in this particular case. Devices infected by AndroidZBot were connected to their remote nodes creating independent botnets. Every botnet consists of tens or even thousands of attacked devices. It means that this Trojan has become a commercial product and is distributed through underground hacker shops, where it can be bought by individual cybercriminals or by organized virus creation groups.

A computer worm program called Conficker deserves special attention. Conficker is one of the most dangerous self-replicating computer programs known. It appeared in 2008, and a year later, Microsoft set a $250,000 reward for anyone who can provide effective information about the virus's creator. The malware exploited a vulnerability in Windows Server Service (MS08-067), where the program occupies a larger memory area than the programmer reserved for this purpose. Thanks to the vulnerability, the program could disable security services such as Windows Defender or system software updates. While working on an outdated system, the virus connected to the server and downloaded the additional malware, allowing subsequent steps, including collecting data from the computer, self-replication via USB and instant messaging, as well as the complete takeover of the victim's computer and putting it under the control of the cybercriminal.

Conficker managed to infect more than 7 million computers around the world. Conficker even infected military systems and most personal computers in Western Europe. It was recognized as one of the top ten computer threats to the Americas by Common Vulnerabilities and Exposures. Conficker was so "successful" malware because its attack vectors were the weaknesses of Windows XP, which was the most popular system in the world in those years. Many devices still work on Windows XP to this day, even though Microsoft has not supported this system for a long time. Despite the passage of time, the virus remains active on many devices. CERT Orange specialists call it a "living archaic

excavation", claiming that they still meet incidents related to the activity of the virus during scanning network traffic.

Conficker also hit Polish cyberspace. It was most active in 2015. At that time, the number of unique IPs from which botnet traffic was generated was 22 899. Thanks to the efforts of Orange Polska, the activity of the virus was limited, and a year later, the number of IP addresses was 9 410. In 2017 – 3 759 IP addresses, and a year later, a slight increase in activity was observed – 4 529 IP addresses.

One of the larger botnets particularly active in Central European countries and the US was a virus with the galactic name "Andromeda". The Andromeda botnet, also known as Gamarue or Wauchos, was first introduced to the public in 2011. Andromeda was a commercial project that consisted of as many as 80 malware families and was modular. It means that cybercriminals created it for sale, and its market price ranged from $ 300-500 in 2011. In 2017, the FBI and Europol removed the botnet from the network. Researchers from Microsoft and ESET have identified over 2 million infected devices in 223 countries worldwide (Sukces FBI…, 2017).

4. Botnets in Poland – An Analysis

In Poland, the phenomenon of an attack using a botnet network is not uncommon. The institution responsible for monitoring threats related to botnet activity is CERT POLSKA. The CERT Polska team operates within the structures of NASK – National Research Institute, which conducts scientific activities, the national .pl domain registry, and provides advanced ICT services. CERT Polska is the first incident response team established in Poland. Thanks to his dynamic activity in the environment of response teams since 1996, he has become a recognizable and experienced entity in the field of computer security (CERT, 2021). One of the team's key responsibilities is to monitor cybersecurity threats and incidents at the national level. Each year, the team publishes an annual report on its activities, which includes, among other things, network traffic from devices infected with Botnet. Attacks using botnets in Poland in the last years covered by the reports were captured and analyzed to compare the scale of the phenomenon in Poland. The analysis covers 2019, 2018, and 2017.

Table 1. The most popular botnets in Poland in 2019, taking into account the size

Family	Size
Andromeda	3 931
Conficker	2 640
Avalanche	2 298
Gamut	1 918
Caphaw	1 563
Mirai	1 520

Family	Size
Sality	1 087
ISFB	723
Nymaim	695

Source: CP Report, 2019.

Table 1 presents the number of infected computers in Polish networks. In 2019, in total, Cert Polska collected information on 635,491 unique IP addresses showing zombie activity. Table 1 shows the highest daily number of unique IP addresses of infected computers in Polish networks. As in the previous year, the Andromeda botnet overtook the rest of the families, despite its infrastructure had been neutralized in 2016-2017. At its peak, Cert Polska registered nearly four thousand infections. At the end of the year, Cert Polska noticed infections of NAS devices of the Taiwanese manufacturer QNAP Systems. On average, there were two thousand of them a day. Compared to last year, the activity of the ISFB and Nymaim banking Trojans decreased almost twice.

Table 2. The most popular botnets in Poland in 2018, taking into account the size

Family	Size
Andromeda	6 059
Conficker	4 529
Mirai	1 969
Sality	1 531
Necurs	1 502
Isfb	1 412
Gamut	1 392
Stealrat	1 312
Pushdo	1 008

Source: CP Report, 2018.

The values in Table 2 indicate the highest daily number of unique IP addresses of infected computers in Polish networks. Cert Polska has observed over 6,000 Andromeda botnet infections daily. Compared to 2017, the number of Botnet Mirai infections decreased more than four times. Conficker has been in the top three largest botnets for many years.

Cert Polska also recorded the high activity of the Marcher botnet. Over 20 thousand unique IP addresses with an Android system were infected with this Trojan in the peak period.

Table 3. The most popular botnets in Poland in 2017, taking into account the size

Family	Size
Mirai	8 334
Andromeda	6 711

Family		Size
Conficker		3 759
Necurs		2 231
Nymaim		1 966
Sality		1 830
Pushdo		1 754
Isfb		1 475
Foxbantrix	Foxbantrix	1 433

Source: CP Report, 2017.

Table 3 presents the number of infected computers in Polish networks. In 2017, in total, Cert Polska collected information on 1,061,670 unique IP addresses showing zombie activity. The values in Table 1 have been established as the largest daily number of unique IP addresses of infected computers in Polish networks. As in the previous year, Mirai came first. It is worth noting that this worm has evolved, and the current implementations differ from those of 2016. Not surprisingly, the high position of the Andromeda botnet, whose infrastructure was neutralized in November, is no surprise. Conficker is in third place, with almost three times fewer infections compared to 2016. Wannacry was out of the top ten; in Polish networks, Cert Polska registered a maximum of 700 infections with this worm in one day.

5. Defense Against Botnets

Botnets are a common phenomenon on the Internet. Any device connected to the Internet can be infected by a virus forming a botnet. There is no universal tool that can effectively and comprehensively protect the device from virus infection. Likewise, there are no vaccines for all the viruses in the world, nor is there a program that can stop all threats.

Botnet defense can be divided into two categories. The first is External Support, i.e., all kinds of antivirus programs and mechanisms of automatic response to threats in cyberspace and systems supporting these processes, e.g., built-in Windows Defender. The second category is related to the user's knowledge and ability to navigate in cyberspace, including knowledge of the basic mechanisms of cybercriminals and limited trust in the Internet. The user who is cautious, preventive, and aware of risks has a low chance that his device will become part of the botnet. An important issue is the education of cybersecurity in schools from a very young age. An educated society is better able to avoid cybercriminals' attacks than one that reacts impulsively and indiscriminately in cyberspace without being fully aware of the many threats.

6. Conclusion and Summary of Research

The threats arising from the activities of cybercriminals using botnets are crucial for maintaining cybersecurity in cyberspace. The very dynamic changes in cyberspace increase the need to pay attention to the problem of botnets. It is not enough just to observe and analyze network traffic and react to incidents. There is a growing need to detect and dispose of botnets at an early stage of their development. It is also important to introduce appropriate protection methods in case of already detected incidents and adapt to the high dynamics of attacks.

The Internet, the cornerstone of cyberspace, has a very vulnerable infrastructure. The proper functioning of the state, organization, and society depends on its security. Botnets are a major threat to individuals, large companies, and corporations. In some cases, there were high awards for revealing the creators of the most famous botnets in the world.

The cases of known botnets analyzed in this article, i.e., Zeus, AndroidBot, and Conficker, indicate a growing trend in cyberspace. The common feature of these botnets is their purpose, which combines the function of stealing money from users' bank account and obtaining sensitive information, passwords and logins. There are many unidentified botnets in the network. Those diagnosed and in part represent more of a historical object than a real threat show the direction of development of cybercrime, and that direction is the new large botnets working in a dispersed structure, difficult to identify, well encrypted, operating in hiding from the user. Each of us can be part of some botnet, even for many years. The most effective defense against botnets is to update knowledge, read carefully and pay attention to the details because, in most cases, the infection is caused by the user.

The analysis of selected botnets in Poland in 2017-2019 showed a downward trend, indicating the high quality of the Cert Polska team's activities. The tables show that in 2017 the total size of all botnets was estimated at over 25,000, and in 2018 by nearly 5,000 less, and in 2019 it also decreased by around 5,000. A smaller number of bots in the network increases user safety. However, it should be remembered that Botnets are not the only serious threat in cyberspace. The analysis of selected cases may indicate better security efficiency and a declining trend of botnets. However, CERT Polska still notices many new botnets, so most likely, the trend related to the activity of "zombie computers" will not be eliminated quickly.

References:

Siwicki, M. (2013). *Cyberprzestępczość*. Wydawnictwo C.H. Beck.

Poulsen, K. (2011). *Haker – prawdziwa historia szefa cybermafii*. Wydawnictwo Znak Literanova.

Kasprzyk, R., Paź, M., and Tarapata, Z. (2015). Modelowanie i symulacje cyberzagrożeń typu botnet. *Symulacja w Badaniach i Rozwoju, 6*(2), 1-15.

Grzelak, M., & Liedel, K. (2012). Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski. *Bezpieczeństwo Narodowe, 22*(II).

Antkiewicz, R., Dyk, M., Kasprzyk Najgebauer, R., Pierzchała, A., Tarapata, Z., and Maj M. (2014). *Koncepcja rozwoju zdolności w obszarze cyberbezpieczeństwa infrastruktur krytycznych państwa, w raporcie Instytutu Kościuszki na temat; Bezpieczeństwo infrastruktury krytycznej wymiar teleinformatyczny*. Warsaw

Hołyst, B., & Pomykała, J. (2012). Group-based cryptography and new challenges to face by computer forensics (part 1). *Prokuratura i Prawo, 11*.

Internet Sources

Analiza bota Zeus. (2011). cert.pl. https://www.cert.pl/news/single/analiza-bota-zeus/

CERT. (2021). *O nas*. https://cert.pl/o-nas

CP Report. (2010). https://www.cert.pl/wp-content/uploads/2015/11/Raport_CP_2010.pdf

CP Report. (2012). https://www.cert.pl/wp-content/uploads/2015/11/Raport_CP_2012.pdf

CP Report. (2013). https://www.cert.pl/wp-content/uploads/2015/11/Raport_CP_2013.pdf

CP Report. (2014). https://www.cert.pl/wp-content/uploads/2015/11/Raport_CP_2014.pdf

CP Report. (2015). https://www.cert.pl/PDF/Raport_CP_2015.pdf

CP Report. (2016). https://www.cert.pl/PDF/Raport_CP_2016.pdf

CP Report. (2017). https://www.cert.pl/wp-content/uploads/2015/11/Raport_CP_2017.pdf

CP Report. (2018). https://www.cert.pl/wp-content/uploads/2019/05/Raport_CP_2018.pdf

CP Report. (2019). https://www.cert.pl/wp-content/uploads/2015/11/Raport_CP_2019.pdf

Czym jest Botnet? (2015). http://cyberprzestepczosc.info/botnet

Kaspersky Lab Polska. (2011). Czym jest drive-by download – poradnik. Infor. https://mojafirma.infor.pl/e-firma/warsztat/269231,Czym-jest-driveby-download-poradnik.html

Keycdn. (2018). What Is a Botnet? https://www.keycdn.com/support/what-is-a-botnet

Maj, M. (2015). *Porozmawiajmy o botnetach*. https://www.cybsecurity.org/pl/porozmawiajmy-o-botnetach-2/

Masywny 13-dniowy atak DDoS botnetu na serwis streamingowy. (n.d.). https://bitdefender.pl/masywny-13-dniowy-atak-ddos-botnetu-na-serwis-streamingowy/

Sukces FBI I Europolu, botnet Andromeda znika z sieci. (2017). https://cert.orange.pl/aktualnosci/sukces-fbi-i-europolu-botnet-andromeda-znika-z-sieci

Trojan bankowy Android.ZBot wykorzystuje wstrzykiwanie www do wykradania poufnych danych. (2015). Dr.WEB. https://news.drweb-av.pl/show/?i=9754&lng=pl

Uwaga! Złośliwe oprogramowanie ZEUS (Citadel/Zitmo). (2016). https://www.bnpparibas.pl/szkolenie/bezpieczenstwo-test/alerty-dotyczace-bezpieczenstwa/zlosliwe-oprogramowanie-zeus

Zeus Report (2011). https://www.cert.pl/wp-content/uploads/2011/01/zeus_report.pdf