Trends of malware influence on the integrated IT security systems at critical infrastructure objects

*Evgenyi Polikarpov*¹, *Alexander Eskov*^{2*}, and *Sergey Anisimov*³

¹Moscow University of the Ministry of Internal Affairs of the Russian Federation, Akademika Volgina, str., 12, Moscow, 117997, Russia

²Krasnodar University of the Ministry of Internal Affairs of the Russian Federation, Jaroslavskaja, str., 128, Krasnodar, 350912, Russia

³Voronezh Institute of the Ministry of Internal Affairs of the Russian Federation, Patriotov, str., 53, Voronezh, 394065 Russia

Abstract. The statistics of crimes in the field of computer information using malware were studied. The analysis of modern types of malicious software is presented in the paper. The trends of the malware market of the anonymous segment of the Internet are indicated.

1 Introduction

Cybercrime is vastly growing and is difficult to investigate. The most prevalent cybercrimes are associated with financial transactions and include bank fraud, carding, identity theft, extortion, and theft of classified information. A significant number of these cybercriminal activities are made with the use of malware.

According to the data from the Ministry of Internal Affairs of the Russian Federation the crimes that involve computers and telecommunication networks make up 11.2% of all crimes from January to March 2019. The rate of the investigated crimes is only 24.13%. The internet fraud forms 8.5%, of which only 21.75% are solved, which is tremendously low in comparison with other types of crimes [1]. The available statistics collected by the Ministry of internal affairs do not disclose methods of committing crimes. However, there is a possibility to estimate the rate of malware using other sources of information and research papers.

The financial institutions have traditionally been the most attractive for the fraudsters. On average every month 1-2 banks lose about 132 mln. rubles as the result of cyber-attacks. As stated by the Group-IB experts the number of cyber-attacks on banks and swift thefts has tripled during the reported period [2].

Automated process control systems are an integral part of the IT infrastructure. These systems include the different range of the hardware and software designed to automate the process control of technological equipment in industrial enterprises. As considered by the experts the intervention of terrorist, extremist and hostile groups in the management of

* Corresponding author: alesc72@mail.ru

automated systems are the main threats for the critical facilities including attempts to disable them completely.

Cybercriminal groups commonly attack industries with the possible high impact on the production and employees such as oil and gas production corporations and energy companies. The tremendous economic and environmental consequences, e.g. disruption of oil or gas supplies, interruptions in the power supply, environmental or humanitarian disasters, could be noticed after the cyber-attacks. The diverse branch networks throughout the country or the world of the transportation companies put them at a high-risk status. Nowadays the managers of such industries pay tremendous attention to the cybersecurity and IT protection. However, the different standardization and approach should be introduced into different organizations based on its requirements. Despite the widespread use of protective software, the unadvised application of the protective measures could lead to a decrease in the overall reliability of the system. Thus, implemented information security tools should be constantly upgraded to provide routine functioning without bugs. So, the industries are constantly searching for the best-fitted solutions.

Moreover, the vulnerability of the critical infrastructure is confirmed by the following examples:

The security systems of the Russian energy giant Gazprom were disrupted by the attackers in 1999. With the help of an insider and usage of the Trojan control of the SCADA-system, that controls the gas supply, was obtained. Fortunately, this attack did not lead to serious consequences, and the typical operation of the system was restored.

The oil production company PDVSA based in Venezuela was attacked in 2002 and the oil extraction reduced from 3 mln to 370 thousand barrels per day as a result of such intervention. Several corporate computers were hacked during the strike of the employees. So, the workers of the company could be possible hackers and leaders of the attack.

One of the well-known and disastrous examples of cybercrimes is the attack on the Stuxnet IT. It was planned and prepared by the Israeli and US intelligence agencies aimed at disrupting Iranian nuclear program.

One of the metallurgical enterprises in Germany was attacked by hackers in 2014. Attackers could not only gain access to the plant management system, but also broke it, causing significant damage to the company. The outcomes of the investigation were stated in the report of the "IT Security in Germany" (Die Lage der IT-Sicherheit in Deutschland 2014), published on December 17, 2014. The attack led to a disruption in the work of furnaces and it's stated in the system as having an "undefined state". Which, as a result, caused significant damage. The attack is already akin as the Stuxnet attack in Iran in 2010.

The same year the attack on Korean hydro and nuclear power Co. was registered. As a result, the information about design and maintenance instructions for several nuclear reactors was snatched. Thus, the company urgently organized workshops on preventing cybercrimes. The panic seized the population of the cities adjusted to the power plants.

The similar cyberattacks happened at the end of 2015 in Ukraine. As a result, more than 600000 inhabitants lost access to electricity. The first emails sent by hackers containing the malware were received by the energy companies six months before the accident. The malicious software (Black Energy 3) provided admission to the passwords and encrypted information about electric networks even though attacked computers were disconnected from the shared system by the IT securities. The hackers obtained the remote access to the operation control systems SCADA after several months of work. Thus, as a result, they could remotely log into the SCADA and turn off the 17 power stations on December 23, 2015.

SCADA systems shifted from the proprietary protocols to the TCP/IP protocols. That is a tremendous achievement for the industries as this system creates more energy, economy and resource-efficient approach to the management. However, the cybercriminal groups are

constantly developing its malware and the vulnerability of TCP/IP protocols is well known. Government and ministries issue new laws and standards for IT security and protection. However, such measures do not allow answering to the hacker's attacks in a sufficient and fast way. As cyber threats evolve tremendously while some of the existing compliance programs provide only snapshots of the security status of organizations and do not allow securing the system in a full.

According to Kaspersky Lab, one of the mainstream threats was targeted attacks in industry in 2017. During the 2016 the number of threats were 20% and this number increased by 7% in 2017. The same numbers (22%) were registered in 2017 in Russia and the growing tendency was also observed. The employees of the Kaspersky Lab ICS CERT prognoses the continuous growth of the attacks and distribution of the malware exploiting vulnerabilities in components of automation systems.

According to the Cybersecurity threatscape (2018) Trends and forecasts research of the Positive Technologies, cybercriminal groups aimed their attacks on the industries while owners of the companies are less informed about cybercrimes and its prevention. It is known that every second industrial company (48%) stated that their knowledge is limited and is less informed about cybercrimes. Moreover, mostly all of them (87%) admitted that they encountered at least one complex cyber incident during the year. Not surprisingly, every third company (34%) spends several days to detect an attack, and every fifth (20%) devotes up to several weeks to find the solution.

Most companies consider the necessity of the appropriate protection against cyber threats and more than half of them (62%) acknowledge the urgency of the complex protective software usage. However, the use of the software is not enough more advanced strategies should be used. So half of the managers (49%) recognize the issue of non-compliance with cybersecurity policies by the employees. Moreover, the mistakes in the industries are more crucial and could lead to instability in the work. Therefore, training in cybersecurity skills is becoming a prerequisite for effective protection.

It is important to notice that the rate of cybercrimes on the industries is about 65%. So the research should be done in order to find the best-fitted solution for protection and sources and pathways of the malware distribution [7].

There were recorded 727 cases of cyber financial crimes using 506 items of unique malware during the September - December in 2019. The most prevalent malware was related to the group of the ransomware, cryptography software that targeted the money or assets collection. Moreover, 540 Internet resources spreading malware were identified and 500 of these resources are registered outside the Russian Federation [3].

The widespread use of ransomware is noticed. Previously, these programs looked alike banners requiring a certain amount of money to gain access to the system. Currently the software encrypts files on a computer and in order to be able to decrypt the files certain amount should be paid. Even the possibilities of the trial decryption are provided. However, the market for such software is vastly growing and the extortionists are more and more sophisticated. In addition, new methods of extortion are developing and using.

The available statistics collected by the companies profiling on information security underscore the relevance of malware threats. Thus, the study of trends in the distribution and modernization of malicious programs allows obtaining comprehensive information on protection system efficiency. In this study, the malware distribution resources, namely trading platforms with easy access to viruses, keyloggers, etc. are analyzed. A research on trading platforms that implement the malicious software shows the most accessible types of such software, distributed countries and number of sold programs as well as its usage etc. As a result, it could provide a comprehensive protection mechanisms and methods and effective analysis of the attacks for the industries.

2 Materials and methods

The most popular sources of the anonymous segment (<https://darkwebnews.com/dark-web-market-list>) of the internet were analyzed. Rate of the prohibited goods and services sold through the dark web is enormous. This is due to the ubiquity of the anonymizers and cryptocurrencies. Above mentioned factors give cybercriminal groups the sense of protection from law enforcement.

Based on the dark web assessment the rate of malware sold through the internet is insignificant. Drug and psychotropic substances traffic is in opposite considerable. Despite the relatively low numbers of the malicious software distribution, the total values are still a matter of concern. Preliminary values are shown in figure 1.

Fig.1. The share of malware based on the trade resources of the dark web

Further research was aimed at malware types. Main trends were identified based on the assessment of fifty trading resources. The total number of advertisements was 2652 not taking into account duplicated ad. The clipper software was least represented with 332 advertisements. The amount of ransomware and Botnet is mostly equal and makes up 390 and 350 accordingly. The number of stealers advertised on the dark web is 525.

Fig.2. Malware type ratios

3 **Results**

The malware Clipper is used to intercept the information about cryptocurrencies wallets during transfers. Clipper abducts the transaction by replacing the initial wallet address with the address belonging to the malware user/creator. Thus, the money is transferred to the malware author, not to the intended recipient.

The concept of ransomware is well studied and consists of the victim's computer data encryption. To restore the access to the data, the ransom should be paid. The type of the malware and its vulnerabilities is of great importance (partially could be found in the description on the website).

Botnet can be used to perform distributed denial-of-service attack (DDoS attack), send spam, and allows the attacker to access the device and its connection and cryptocurrencies mining.

Information stealers are located on an infected computer and collects data (credentials used in online banking, social networks, emails, etc.) for the hackers.

The key factors of the studied malware are its popularity, ratings and sales in the assessed information environment. The most popular malware is stealer (on average 350 views and 120 purchase). The total of 300 views and 95 purchases were registered for the clippers. The ad frequency on ransomware is quite diverse as such viruses are very popular and cheap. On average number of views is 280 and the number of completed purchases is 70. Also, should be noticed that more cheap versions of the ransomware are the most popular among buyers.

The Botnet types are also quite popular and differ in specifications due to the possible number of affected nodes and number of views is 250. The amount of purchases is slightly bigger than in case of ransomware and makes 90 purchase mostly for the Botnet types with the greater number of affected nodes. The above-mentioned features are shown in figure 3.

Fig.3. Popularity of the malware

The last step during the research was malware cost assessment. Based on the collected information the median cost of the ransomware ranges from \$0.50 to \$3000 depending on the specifications. Moreover, the price varies greatly as the sellers provide not only a one-time purchase but allow the buyer to subscribe for a month or even a year. Ransomware could be bought for \$16 (0.0313 BTC) on the WallStreet site. The price for the Clipper varies from \$6 (0.0011 BTC) to \$40 (0.0076 BTC). Average fee for stealer is \$15 (0.0028 BTC). The Botnet cost depends on the specification and number of the bots and varies from \$25,75 (0.0049 BTC) to \$4500 (0.85 BTC). The sellers declare the quick payback on their services and goods as average ransom for data encryption lays in range from 0.037 BTC to 0.092 BTC (\$200 - \$500). Consider the price and payback the ransomware availability is immense. The cost ratio is shown in figure 4.

Fig.4. Cost ratio of the malware

4 Conclusion

Analysis of the software illustrates the great availability and reasonably low costs of the different types of malware. Such results, in turn, shows the possible threats for cybersecurity. The research noticed the necessity of the cyber-crimes prevention and determines the main trends. Based on the data the unsatisfying forecast could be done:

The less protected critical IT resources would be attacked. The companies without proper cyber protection are in the high risk. Main threat is the use of malware.

New ways of the malware distribution and improvements of the old versions would be prevalent.

The launch of the new malware would be based on the social engineering methods.

Cryptographic programs remain the most efficient and fastest way to make money from cybercriminals.

The diverse malware market would allow conducting serious attacks even by the unskilled hackers.

Key factor of the malware distribution is the popularity of the dark web. More and more cybercriminal groups prefer to buy complete solutions instead of investing in the development. As a result, similar software is going to be used by the different groups.

Developers would benefit from selling the same copy to different customers. So, the malware would be targeting a wider audience. Extensible modular software with flexible architectures would be of a great priority. It goes without saying that such universal malware will be more popular among hackers than niche tools.

Prevention of the mentioned malware attacks could lay in the optimal and balanced configurations of cybersecurity tools. Moreover, the local virtual environments and systems (sandboxes) with their subsequent investigation of the resistance to the described malware should be created. Industrial enterprises should develop a comprehensive strategy to prevent attacks using malicious programs.

The most significant step in the cybersecurity is a precisely managed security plan and assessment of the potential cyber risks. It should be noted that not only external threats to cybersecurity should be taken into account, but also internal flaws as a result of the inappropriate use of the software and the lack of personnel awareness.

Firstly, the cybersecurity starts from the people. The next step in preventing malware in industry is coaching and education of the personnel, providing up-to-date information about cyber-crimes and security.

Adaptive IT security technology should be used in the constantly changing cybercrimes environment. While putting an additional level of protection, the level of malware attacks could be drastically reduced.

In conclusion it should be noted that prevalent malware is designed to bypass common protection systems. In order to prevent cybercrimes, the holistic approach should be used. An effective cybersecurity starts from developing efficient strategies by the CEO, not by redirecting the issue on to an IT manager or a security officer.

It is significant to use multi-layered solutions that are diverse in protection and would allow maintaining a sustainable environment at such industrial facilities.

References

1. Characterization of the state of crime in the Russian Federation 2019. The site of the Ministry of Internal Affairs of the Russian Federation, <https://www.mvd.ru>.
2. S. Petrov, V. Alpatov, *MATEC Web of Conferences* **106**, 04002 (2017). DOI: 10.1051/mateconf/201710604002
3. V. Y. Alpatov, A. A. Sakharov, O. Y. Veremeenko, A. A. Lukin, *MATEC Web of Conferences* **86**, 02021 (2016). DOI: 10.1051/mateconf/20168602021
4. The site of the company Positive Technologies, <https://www.ptsecurity.com>.
5. E. Butorina. *Encrypted Spying* (2019).
6. W. Strielkowski, E. Volkova, L. Pushkareva, D. Streimikiene, *Energies* 12(7), 1392, (2019). DOI: 10.3390/en12071392