CYBERCRIME EVOLUTION

Mircea Constantin ȘCHEAU*, Ștefan Zaharie POP**

**“Alexandru Ioan Cuza” Police Academy, Bucharest, Romania

***“Nicolae Bălcescu” Land Forces Academy, Sibiu, Romania

mirceascheau@hotmail.com, popstefan2000@yahoo.com

Abstract: *Information as a structure has changed. Database architectures can hide executive models or constitute simple, manipulable packets form. The transmission of information has undergone mutations dictated by technological evolution, and intercepting methods have proven the capacity of adaptability and penetration. The term "cybercrime" may appear to be abused, but if we look more closely at the global phenomenon, we will understand that all levels of human society are affected without distinction. Starting from the environmental conditions that can be improved, the energy, industrial and transport sectors that can be much better coordinated and reaching the missile fields that can be hijacked, we understand that all depend to a greater extent or less of the aggressor's ability, the preventive and reactive measures implemented, and the degree of resilience that can be provided by defensive or offensive defense structures.*

Keywords: attack, vulnerability, cryptocurrency, infrastructures, globalization

1. Introduction

The new Internet of Things (IoT) era is in full assertion, and any infrastructure that is developing will have to relate to the entire process chain risks developed. Causality may encapsulate superficiality, corroborated with faulty resource management and a lack of adequate investments. The misunderstanding of the needs of the decision makers finally leads to the recording of losses that will not allow an immediate recovery. Cybercrime is not a threat – it is a reality. Black hat hackers activity must be regarded as any profession that requires special abilities, hard work, and a lot of perseverance. In order to understand the offenders and to debunk what we do not want to accept, it is enough to look for the motivational factors and we will find that they are much closer to human nature than we imagined at the beginning. Any modernization project involves the insertion of programmable

elements and therefore, exposed to cyber aggression. Critical infrastructures include interdependent sectors and subsectors. A blocking or syncope in operation give rise chain reactions in the situation where there is no clear functional segregation, addressability and responsibility. The crime industry benefits from generous funds and state support. Cryptocurrencies offer one of the anonymity umbrellas indispensable for the incubation and implementation of plans and add to traditional methods. Comprehensive amounts allow the acquisition of difficult to purchase materials from the civilian environment, allow the financing of a complex operation, or can be used as a takeover a competitor tool or as a weapon to destabilize a region.

It is no surprise that the US Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) reported at the end 2018 that for several infrastructures there is imminent danger of conducting

computer-related attacks [6]. Ensuring good security requires close collaboration with the private sector. There is nothing new in what I have said before, but the message must be repeated until the government – private symbiosis will allow for the necessary involvement that will lead to overall distributed awareness. The relationship should be multilaterally developed and support from private companies needs to be reflected in state support. Government regulatory authorities should cooperate with expert groups to develop standards. Regulation can lead to prevention seen as early detection. Recovery depends among others proactive measures and instruments developed for this purpose. Risks and potential damages assessment is also part of the prevention and ensuring the independence of reports provides clarity to the images.

2. Cryptocurrencies and cybercrime

Cybercrime has no borders. It makes its presence felt particularly in areas where legislation is permissive and tacit collusion or intensive collaboration between crooks and state bodies allows the creation of enclaves from which to launch the actions. More cells lead to a multicellular carcinogenic organism with replication and regeneration properties. The export of crime has transformed itself as a different notion and has been split because state actors possess the necessary financial instruments needed to disguise erosion operations in the form of respectability. Cryptocurrencies have appeared and developed apparently as a form of protest against the traditional financial system, but it turns out that some of the branches created only aim to support illegal actions or military strategies. The reason for the blockchain technology is now a pretext for the development of many conflicts. Innovation provides many applications that generate added value but some results of the same innovation can be used in a

destructive way. The cybercrime globally speed propagation is much higher than the speed of globalization at the social level. If in the case of states, there are efforts to identify the levers needed to eliminate intercultural issues, in the case of cybercrime the offensive actors have no any communication problem. The languages are the same, the platforms are the same, and most often the interests are the same.

It is no longer a secret that after the action of a ransomware that encrypted the data, it almost invariably follows the demand for redemption in one of the consecrated cryptocurrencies. The victim has to decide if agrees/ or not to pay. We are not just talking about individuals. Companies, institutions, or simple organizations are just as vulnerable. The decision involves balancing settlement amount versus encrypted information. The average amount of redemption has increased due to the willingness to pay, and everything is transposed into a continuous loop that drives new resources. Some attacks are the work of people hungry for recognition or money [10], but others are thoroughly prepared and orchestrated to hide its real intentions. In none of the cases there is certainty related to the recovery of the information. Moreover, when the exchange cryptocurrencies is acquired or when it is transferred to the claimant, it is possible that a man-in-the-middle diverts the funds and thus the victim runs out of money and data compromised. The warnings from the specialized companies are conclusive and it is preferable that the advice be followed before it is too late [3].

Insurance companies can easily become victims of delayed decisions and there are cases where the financial effects were important. This is added the lack of information specific to employees from different geographical areas and the unprofessional approach to real threats. Misalignment of the standards within the same multinationals company makes the

success achieved to be counterbalanced by the losses in other areas.

Significant material damages is difficult to be accepted, but human ones are inadmissible. That is why the measures adopted to improve information security, for example in the UK healthcare sector, have as their stated aim to prevent and combat cybercrime through more careful planning and an increase in resilience degree. WannaCry has disabled the national healthcare systems and affected more than 3,000 computers in hospitals, encrypted stored data, and interrupted hundreds of medical procedures in just one month during 2017. Patient safety has been jeopardized and any amount required to unlock workstations does not justify the possible loss of human lives [2].

Voices with authority in the field at the international level have drawn attention to the many dangers generated by the lack of regulation of cryptocurrencies and the possibility that investors' good intentions may be exploited to support projects located far outside of the law. Concerns do not refer to the technology itself, but to the way it is used. Fuelling speculative bubbles and engaging support groups have prompted specialists to position themselves realistically against new trends, warned public opinion about embezzlement practices, and directly accused craftsmen behind the curtains. The threats from newstream proponents of cryptocurrencies were followed by concrete actions of attack, which in fact confirmed the idea of linking cryptocurrencies with cybercrime or even cyber terrorism [5].

Both need tools and resources. That's why attackers have focused on exploiting the computers or intelligent phones without the knowledge of the owners and one of the examples is the Teror Exploit Kit, which was discovered at the end of the year 2016 and which had as its main objective the transformation of infected systems into mining units of cryptocurrencies. Another cryptojacking attack vector was used for the

same purpose of mine in the fourth quarter of 2017 and aimed at unauthorized scripting in browsers. The trend changes according to profitability. Exploit kits are the most accessed malware delivery mechanisms and can be directed to mining or spreading [1].

Cryptocurrencies have become favorites in the rankings of exchange units, which has increased the risk of attack on trading platforms. Ransomware and / or zero-day vulnerabilities are used to take control of storage wallets [7], and spam campaigns using JS.Downloader and / or Microsoft macro (W97M.Downloader) incorporating additional functionalities further enabling them to steal Bitcoin. The orientation was explicitly directed towards a virtual currency with a value exponential evolution [8]. Cryptocurrency has become target and instrument of attack at the same time and behaves more like a commodity or a bearer of securities whose quotation changes abruptly according to the signals transmitted by the regulated financial markets and the positions of officials who fight or encourage phenomenon. Increasing the value of certain cryptocurrencies draws on itself the appetite increased, which leads to a new incrementation and thus the bullets begin to roll. The simply crime grows and by becoming a business, it claims its place to fall naturally into the perimeter of the crime industry.

Given that blockchain technology has enough applications in various domains, computer-based aggressors believe they have identified the ideal transfer element in cryptocurrency, and the specialists [9] have some directions that are highly resolute in the cybercrime environment and against which we have to focus our attention in 2018. Artificial Intelligence (AI), Machine Learning (ML) and IoT devices will be used much more often he construction of actions, state attacks will become more numerous and more robust, the number of malware will have a growth rate faster than before today, financial trojans will cause greater losses than ransomwares, etc.

Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and in particular Software as a Service (SaaS) will also increase the number of vulnerabilities.

3. Combating cybercrime

At the each State level there are strategies to combat cybercrime, and in the case of the European Union, efforts are being made to bring about uniformity, in keeping with certain specificities. The dangers are multiple and besides those of an economic or military nature, they are also of an individual nature. The access to personal data may provide access to everything means private or / and public life. The General Data Protection Regulation (GDPR), which is the date of entry into force in May of the year 2018, sets fines for companies that fail to adequately access data access staff of the citizens of the European Union. It is a mandatory stage to consider if it is desired to protect the individual and his credentials. Banking financial institutions, private companies, or any other entities in which the person is operating, including military units, may be infected by contamination. The immense world of the Internet offers conducive conditions to the exploitation of human vulnerabilities and and taking advantage of them in order to sabotage the active fronts of defense architectures.

In order to cope with aggressions, an effective security strategy and a framework to support immediate reaction actions is needed. Remember a few recommended measures [4] to prevent potentially dangerous situations:

- double checking - collecting information on particular non-core mechanisms and functionalities and confronting the results;
- articulation of the necessary adjustments - customizing each decision according to the environmental conditions in order to create a perfect balance, safety oriented;

- identifying all potential risks - cyber threats are changing according to technological evolution;
- the unification of security controls - the time factor can prove to be crucial in case of high penetration attacks;
- the using of the latest innovations - the improvement of the strategies depends to a great extent on the implementation of the appropriate techniques and adapted to the immediate realities;
- specialized back-up - to support efforts, it is advisable to have the possibility to appeal to ultraspecialized teams, external to the organization.

Of course, all these recommendations are only a few of the surface ones, and therefore each organization will develop its own defense and control mechanisms. The specifics of the activities and the prioritization of the tasks will be the ones that will ultimately decide.

4. Conclusions

It is difficult to expose in some lines the general evolution of cybercrime because its development occurs horizontally and vertically. Depending on the purpose, the final target may be singular or may consist of fragments located at several points of the globe. We believe that an increase in the awareness of the entire population will support the efforts to combat the criminality. Education starts from the earliest age and addresses equally elderly people. Public private partnerships can also induce vulnerabilities, but good management of the phenomenon may provide the right answers to any challenge. The boundary between online freedom and criminality remains a subject under discussion, but in the case of national security, which includes, among other things, economic stability capable of providing military response capability, we believe that, with regard to the general interest versus the individual interest, the opinions are converging and support the idea of a common front against aggression.

References

- [1] ENISA - Threat Landscape Report 2017, 15 Top Cyber-Threats and Trends, 2018.
- [2] <https://www.aig.com/knowledge-and-insights/k-and-i-article-state-of-cybersecurity-uk-middle-east-africa#>
- [3] https://hotforsecurity.bitdefender.com/blog/bitcoin-hijack-steals-from-both-ransomware-authors-and-their-victims-19525.html?utm_source=SMGlobal&utm_medium=Facebook&utm_campaign=H4S
- [4] <https://www.itproportal.com/features/cyber-security-deployment-guide-to-effectively-safeguard-systems-data/>
- [5] <https://www.rt.com/business/418790-doom-roubini-crypto-crazies-terrorists/>
- [6] <https://securityboulevard.com/2018/01/an-infrastructure-plan-in-the-21st-century-needs-to-address-cybersecurity/>
- [7] <http://securityaffairs.co/wordpress/69100/hacking/bitmessage-zero-day.html>;
- [8] <https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-ransomware-2017-en.pdf>
- [9] <https://www.symantec.com/blogs/feature-stories/2018-cyber-security-predictions>
- [10] https://www.theregister.co.uk/2017/04/25/british_malware_author_2_years_jail_titanium_stresser/