CYBER CRIME – CHALLENGES AND EVOLUTION

Mircea Constantin Șcheau*
National Bank of Romania

Abstract

The notions conveyed in the media, regarding the approaches to cyber threats, are sometimes placed under the pressure of step-by-step transformations, subject to the mechanism known as Overton Window. The article tries to bring to the attention of the public opinion and to the same extent of the specialists, some of the hybrid problems whose escalation can produce effects difficult to be quantifyed. The set of proposals from the end of the study are intended to be a pleading in support of the idea of interinstitutional cooperation and active involvement of civil society.

Keywords: financial institution, vulnerabiliy, malware, cyberattack, infection vector, impact, coordination.

Clasification JEL: F60, H56, K24, M15, O33.

Introduction

A simple overlooking of the current state of affairs shows that the subject raises interest in the context in which the relationship of dependence between society and innovation becomes more and more evident. It would be a mistake to assume that there are completely isolated infrastructures and to think only to particular associations of specific terms with computerized subdomains. Interoperability involves interconnectivity, automation, and not for few times, remote control systems. Devices whose exploitation is accessible to the domestic environment are used for real-time monitoring and allow addressing resources with a regulated status or belonging to a zone classified as a dark component (e.g. dark web). In a simple smartphone, technology is more advanced than in a spaceship in the 1970s.

* Author for contact, **Mircea Constantin Șcheau**: mirceascheau@hotmail.com

The opinions expressed in this article belong entirely to the author and do not reflect the official position of the National Bank of Romania.

In the view of actors who are faced with each other on multiple plans, escalating economic conflicts to seize market shares justifies calling for procedures that could easily fit into the gray area of international law. Research laboratories and strategic teams are the main targets of competitors. Virus strains are reinvented to bypass protection solutions. Modern techniques complement old-fashioned manipulations.

Financial crime and the necessary activities to combat it are different from those associated, for example, to cybercrime in telecommunications, but intersection points and overlapping areas call for measures to respond in a coordinated manner to aggression. In an anonymous poll of over 700 security professionals in the UK, Australia, the United States, Mexico, Germany and Japan, nine out of ten respondents said the organization they worked for was "successfully" affected by at least one cyber attack between 2016 and 2018 and approximate half of the attacks resulted in the recording of some non-functioning intervals of critical considered systems [4].

I believe that one of the major problems faced by security structures for a long time is generated by a lack of culture of ordinary consumers, the tangible impact reflected in personal data exfiltration, compromising credentials and, implicitly, possible financial losses. The apparent security, dismantled without too much effort by black hat hackers or gray hat hackers, reveals vulnerabilities classified at first instance as harmless. An expert group discovered at the end of 2018 that exist malware that actively scan Web services and Internet-connected devices [16] to discover possible exposures and default passwords. The Xwo Python script, linked to malware families previously known as Xbash and MongoLock, combines different features, specific ransomware, cryptocurrency miners, worms, backdoors etc. Malware has been attributed to a criminal group, Iron Group, whose activity has been reported since the beginning of 2016.

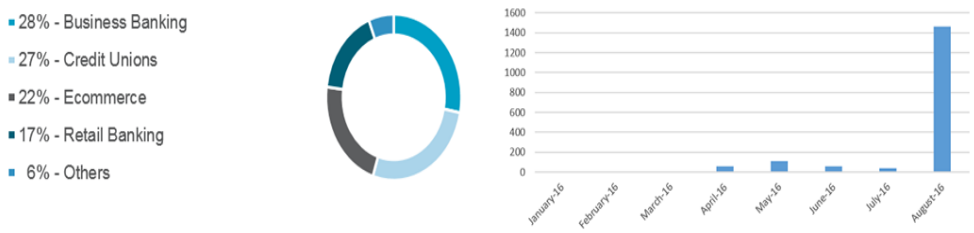


Figure no. 1. The GozNym effect [8], [9]

Viruses that have affirmed themselves globally, malwares which have reached the expectations of the initiators and have gathered a sufficient number of appreciations to be declared successful will never be abandoned, no matter of the security methods developed by security teams against. Their reinvention align with the new technological realities. The source code is modified, combined with other source codes and adapted to bypass improved firewall versions. Preferred targets will be the same on which the maximum effect was recorded or adjacent to them. An eloquent example is the Trojan originally discovered in 2007 and involved between 2016 and 2018 in strong campaigns against financial banking institutions, insurances companies and not only. GozNym combines the features of Gozi ISFB and Nymaim. On the right side of the picture in figure 1 are detailed the sectors affected

in 2016 in North America and on the right side the activity in Europe [8], [9]. In 2018, Gozi (Ursnif) ranked first in the list of most active financial malwares after a third place occupied in 2017.

Another example is Kronos banking Trojan, whose new variant targeted more states in 2018, the main improvement being the Command & Control system, which used the Tor anonymization network. Even if a re-labeling was attempted under the name Osiris, the similarities with the old version are obvious: the same WebInject format, Zeus malware format, the same protocol and C & C encryption mechanism, extensively overlapping codec and last but not least 350 Kb size, comparable with the 351 Kb of a previous version [13].

Also in the context that we referred to, an underminer exploit kit created at the end of 2017 and released in early 2018 delivered a bootkit and a cryptocurrency-mining malware generically called Hidden Mellifera, and included asymmetric encryption functionality, URL randomization etc. [14].

Another banking Trojan, known as BackSwap, appeared in March 2018. Even though it has novelty elements related to WebInjection, its features are very similar to those of another Trojan known as Tinba. The way of action highlights the importance of authorization and authentication mechanisms, with the negative effects being more successful in the situation of institutions whose structures of protection did not respect international standards in the field. A suggestive image presents a list of the top ten financial malware, noting that this ranking may differ, depending on the company that conducted the study [10].

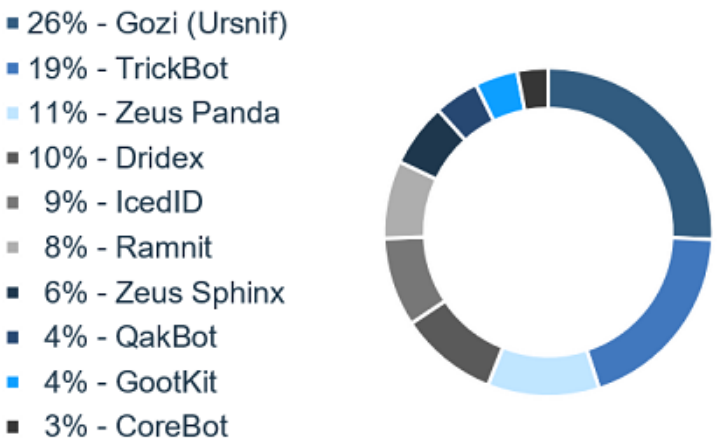


Figure no. 2. Most relevant families of financial malware in 2018 [10]

Another interesting episode was the relaunch of the Ratopak / Pegasus spyware, known to be engaged in 2016 in attacks against financial-banking institutions. It was announced in underground forums that it is a new version containing the source code of the malware used by the Carbanak group, but ultimately was assigned to the Buhtrap group, the decision being determined by the identification of a signing certificate that appears in binary code and which was used in the aforementioned aggressions. The action mode, the use of a sideways module,

a customized, updated version of Mimikatz to "harvest" credentials, the injection of the code through "WriteProcessMemory" technique, PowerShell broadcasting, SCM, WSH Remote or RDP Scripts, different techniques which provide the ability to run a script on a remote machine and take control of it, are just some of the high-similarity features identified by researchers [15].

The above-mentioned ones induce the idea that the financial area is the predilect target of the attackers and must be given due attention. It can be simply assimilated to sectors for which protection and stability have to be ensured.

1. Transformtions and Responses

In order for transactions to become safer, whether we talk about modest payment orders or international transfers subject to a standardized regime, efforts are being made to identify solutions that will lead to the consolidation of defense blocks. Biometric authentication methods were considered safer until millions of profiles began to be sold on the black market with prices ranging from five to several hundred US dollars. At the beginning of 2019, a cybersecurity company that has been operating for more than 21 years, has published the results of an investigation into the sale of about 60,000 units via an online Genesis Darknet marketplace. Access was based on an invitation and were offered to the buyers all the information they needed to use the products [7]. Crime-as-a-Service (CaaS) is no longer just an expression in a dictionary. Malware trunks can be concatenated, it is possible to gain access to customer databases for whom the weak points are known and accurately indicated, zero-day vulnerabilities can be auctioned, or can be "hired" teams ready to perform malicious work against a private or governmental target. The palette is quite wide, from custom viruses to living-off-the-land (LoTLs) or shared criminal infrastructures. Are underground markets in continuous development, because supply is correlated with demand also in this case.

Of course, the level of protection can be increased and there are companies willing to invest in constructions capable of processing complex functions. Machine Learning (ML) is no longer an unknown. It is stated as an important branch of Artificial Intelligence (AI). As an example, we can refer to the primary identifying elements of a person, who are loaded into information processing systems. Behavioral analysis, involuntary gestures during the crossing a monitored aisle, facial expressions, reactions to external stimuli, or vocal fragments is the classified basis by categories from which it starts. All of these are compared to real-time ML sequences and corroborated with those injected later by the human operator. Any inadvertently sends an alarm signal to the surveillance team, which decides whether the impulse should be assimilated to the original or shall immediately applied the stipulations of the security plan.

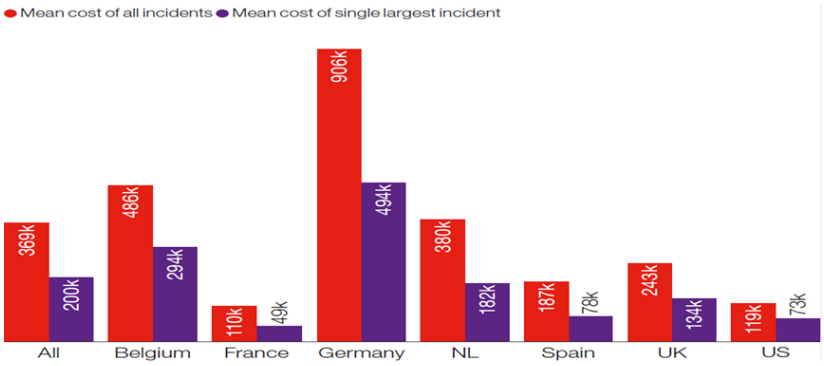
It is indisputable that periodic assessments are particularly useful in identifying internal security policy weaknesses and contribute to updating existing programs. Red team and penetration tests can provide an overview of the key objective of assessing the effectiveness of detection, prevention and response capabilities. A phishing email produces residual proofs and direction are sometimes oriented to social engineering scenarios based on harder-to-detect calls. As an example, after studying the client's infrastructure and its connection to the online public environment, can be clone the authentication portal and even fake the entire

structure, including the IT support phone number. An information is sent according to which emails have been migrated to a new server and employees are required to connect to the cloned OWA portal. To avoid any suspicion, comunications are immediately redirected after authentication to the legitimate OWA portal, but using this method red team captures enough credentials to establish a support point in the internal network. The compromising of privileged accounts, corroborated with the lack of judicious segmentation, provides full access in a short time [1]. Such exercises are recommended to be performed simultaneously for all connected structures. Can be highlighted common and particular vulnerabilities, including those that can migrate.

Industry	Users Targeted (%)
Mining	38.4%
Wholesale Trade	36.6%
Construction	26.6%
Non-classifiable Establishments	21.2%
Retail Trade	21.2%
Agriculture, Forestry & Fishing	21.1%
Manufacturing	20.6%
Public Administration	20.2%
Transportation & Public Utilities	20.0%
Services	11.7%
Finance, Insurance & Real Estate	11.6%

Figure no. 3. Malicious Email per User by Industry [3]

Under ideal conditions, detection of malware is impossible, and the presence can only be signaled due to the effects. This involves the occurrence of losses in the interval between the time of the infection and the implementation of the solution [5]. Victims can be simple users, multinational companies or state organizations: ministries, military intelligence agencies, energy producing groups etc. No one should consider themselves fully protected. Anyone can be attacked directly or through a third party collaborator. The risk of contamination is quite high. The same infection vectors and the same techniques can be used for different environments, as can be seen from the statistic in figure 3, valid for 2019. Web platforms are used more intensely and environments with pre-installed systems are much more accessed because it is difficult to be identified the operators behind the action.



Mean cost of all incidents by sector ($)

	Pharma and health	Travel and leisure	Financial services	Transport	TMT
2019	726,000	703,000	628,000	530,000	464,000
2018	103,000	148,000	400,000	157,000	349,000

Mean cost of largest single incident by sector ($)

	Pharma and health	Travel and leisure	Financial services	Transport	TMT
2019	388,000	427,000	301,000	229,000	288,000
2018	11,000	29,000	83,000	38,000	52,000

Figura nr. 4. Costul mediu al incidentelor cibernetice ($) [6]

It's predicting a $ 1.5 billion increase obtained from cybercrime profits and reaching the 70% threshold by 2021 from the volume of cryptocurrencies allocated to the underground industry. Losses will exceed $ 6 trillion annually, under the circumstances than 146 billion registrations expected to be exfiltrated by 2023 [3]. The financial impact, total cost, frequency and intensity of attacks increase and implicitly must be incremented the level of information and training. Although there are differences in cybercrime losses, a study highlights common issues surrounding the prevalence of attacks and the cost of recovery [6]. In the present case, the interest indicators of the aggressors represent short, medium and long-term projection landmarks. The reports are dynamic and the graphs can record medians with different values, making it even more difficult to draw the predictive coordinates.

It is true that the rise of Artificial Intelligence / Machine Learning now allows for accurately examining and identifying the coding style of a person or even a group of people who work together on the same project, but the outcome may be more useful in reactive sense than anticipatory. Even if standardization or unanimous acceptance of an established method can not be discussed, anonymization and plagiarism abot programming may soon become just a theoretical phrase. Tests revealed that the level of experience of an IT engineer, in combination with the number of products developed and their degree of difficulty, is directly proportional to the degree of precision of his identification. Specifically, the more experience an IT engineer has, the more he participated in the construction of more products, and the higher their difficulty was, the higher the percentage of accuracy of unveiling his anonymity. Stylometry claim itself to be a sphere of activity that can be embedded in several subdomains, with the answers being some of the most surprising [11]. Computer security enthusiasts, who have developed their skills and are willing to make an effort that meets the challenges,

sometimes need only a few clues to help them formulate a 'Kickback'counter. Depending on the aggression, after identifying the starting fragments, the approach strategy is being implemented together with the law enforcement agencies [12].

Conclusioan and Proposals

Viewed from outside, scenarios can be perceived as apocalyptic and looks more like science-fiction novels than cruel reality. And the criminals rely on that. On the feeling that " It can't happen to me" or " Why should it happen to me if I do not show any interest to anyone?". Each of us can become a simple piece in a GO game or we can be attracted in a whirlwind of geometric figures that change their shape and placement continuously. All we can do is not give up for a second trying to prevent and change the mentality of those around us. Twenty years ago we use to lock the door with the key and opened it only to people we knew. Not so long ago, when we only knew the currencies we could buy ordinary goods with, we didn't think the time would come when cryptocurrencies would try to impose themselves as an alternative. But the lack of regulation in the field favors the underground economy and without coherent policies, it is difficult to be combated the criminal phenomenon. The border of cybercrime can be considered to be synonymous with the limit of imagination, and in this case, it is good to be aware as soon as possible that the aggressors, who once upon a time attempted to invade our personal space through crude methods, now can do this invited even by us.

Each manufacturer recommends updating as part of the product security enhancement processes or preventive vaccination, metaphorically speaking, and changing initial passwords with some that meet length criteria and key combinations, thus lifting a first barrier to attackers. The Internet of Things (IoT) is basically the support for Internet of People (IoP) and together evolving rapidly to the Internet of Everything (IoE). Wifi Protected Access (WPA), a protocol launched by Wi-Fi Alliance to authenticate connected devices without physical data transmission support (wireless) using the Advanced Encryption Standard (AES), has been shown to have security flaws, despite the increase in cryptographic power and in the conditions that it becomes increasingly difficult to separate personal by professional activity, a company can easily become a victim. An attack could be successful with the help of an employee who does not properly treats a phishing email or violates another internal security rule. An episode of this kind may be categorized as a human failure. In these circumstances, specific motivations must be valued to narrow the penetration channels as much as possible and to reduce the areas exposed to possible aggressions. The rationales for increasing degree of risk intolerance must be placed in the foreground and sustained.

To resist competitive pressure, companies need to understand disruptive trends with a clear influence on markets, on customer behavior and expectations, as well as on employees. Growth opportunities stimulate efforts for modernize infrastructure and open new perspectives for digital transformation. Are established priorities in the construction of an innovative culture and in this context, must be recognized the special importance of the human factor in the development of cross-border collaborations [2].

At European Union level, it is necessary to set up joint working groups to analyze and elaborate best practice for each area or ministry in order to be implemented, calendar basis,

alignment measures to the same standards. Calls addressed to primary support services or teams prepared to respond to computer-related incidents, even those from the civil area, should be supported throughout the European Union, be monitored and reported in such a way as to lead to a faster identification of attack patterns and of aggressors. The concept of a (secure) communications structure with European coverage, with a centralized Artificial Intelligence system or managed on modules, can be developed only in the conditions of legislative unification, which to set the exchange of inter-institutional, interstate information and the model of collaboration between service providers and authorities [17]. In this context, fast forwarding to competent bodies of information on any cybercrime event is vital to ensuring resilience and must be a priority for official bodies or private legal entities regardless of the industry in which they operate.

In order to implement the above proposals, I also believe that it's necessary to be initiated at European level, in the educational environment, a concept of familiarization with the primary notions of computer security and even of their deepening. In addition to the general information programs held in public-private partnerships, starting from the gymnasium cycle until the completion of the average, high school courses, the school curricula should allow the inclusion of chapters specific to this topic. A well-informed society as a whole can react to aggressions and contribute actively to limiting and even preventing losses.

About the author

Mircea-Constantin ȘCHEAU is PhD in Public Order and National Security with a theme of interest for the economic and security domains - *Cybercrime regarding Financial Transfers*. Author and coauthor of three books, more than twenty scientific articles in the field of management, economy, law enforcement, defense, critical infrastructures, information technology and lector to many international conferences.

Acknowledgement

The opinions expressed in this article belong entirely to the author and do not reflect the official position of the National Bank of Romania.

The original article was published in English in the study "Considerations on Challenges and Future Directions in Cybersecurity", ISBN 978-606-11-7004-3.

Bibliography

[1] A. Rahman and C. Antolik, "Finding Weaknesses Before the Attackers Do," *Threat Research*, FireEye, 08 April 2019. [Online]. Available: https://www.fireeye.com/blog/threat-research/2019/04/finding-weaknesses-before-the-attackers-do.html.

[2] B. Solis, "Seven Priorities To Accelerate Digital Transformation Maturity and Success," Forbes, 09 January 2019. [Online]. Available: https://www.forbes.com/sites/briansolis/2019/01/09/seven-priorities-to-accelerate-digital-transformation-maturity-and-success/amp/.

[3] C. Crane, "80 Eye-Opening Cyber Security Statistics for 2019," The SSL Store, 10 April 2019. [Online]. Available: https://www.thesslstore.com/blog/80-eye-opening-cyber-security-statistics-for-2019/.

[4] *D. Simmons,* "Cyber-attacks 'damage' national infrastructure," BBC News, Technology, 04 April 2019. [Online]. Available: https://www.bbc.com/news/amp/technology-47812479.

[5] F. Cohen, *Computer Viruses - Theory and Experiments*, Computers & Security, vol. 6, pp. 22—35, 1987.

[6] Hiscox Ltd, "Hiscox Cyber Readiness Report 2019," [Online]. Available: https://www.hiscox.com/documents/2019-Hiscox-Cyber-Readiness-Report.pdf.

[7] Kaspersky Lab, "Kaspersky Lab uncovers Genesis: The underground e-shop with tens of thousands of digital doppelgangers for sale to bypass financial anti-fraud solutions," Press Release, 09 April 2019. [Online]. Available: https://usa.kaspersky.com/about/press-releases/2019_kaspersky-lab-uncovers-genesis-new.

[8] L. Kessem, "GozNym's Euro Trip: Launching Redirection Attacks in Germany," *SecurityIntelligence*, IBM X-Force, 23 August 2016. [Online]. Available: https://securityintelligence.com/goznyms-euro-trip-launching-redirection-attacks-in-germany/.

[9] L. Kessem and L. Keshet, "Meet GozNym: The Banking Malware Offspring of Gozi ISFB and Nymaim," *SecurityIntelligence*, IBM X-Force, 14 April 2016. [Online]. Available: https://securityintelligence.com/meet-goznym-the-banking-malware-offspring-of-gozi-isfb-and-nymaim/.

[10] L. Kessem and T. Agayev, "BackSwap Malware Now Targets Six Banks in Spain," *Analysis and Insight for Information Security Professionals, Security Intelligence*, IBM, 22 August 2018, [Online]. Available: https://securityintelligence.com/backswap-malware-now-targets-six-banks-in-spain/.

[11] L. Matsakis, "Even Anonymous Coders Leave Fingerprints," Wired, 10 August 2018. [Online]. Available: https://www-wired-com.cdn.ampproject.org/c/s/www.wired.com/story/machine-learning-identify-anonymous-code/amp.

[12] M. Ramilli, "Hacking The Hacker. Stopping a big botnet targeting USA, Canada and Italy**,**" *Cyber Crime, Hacking*, Security Affairs, 31 August 2018. [Online]. Available: https://securityaffairs.co/wordpress/75782/cyber-crime/hacking-hacker-botnet.html.

[13] P. Paganini, "Kronos Banking Trojan resurrection, new campaigns spotted in the wild," *Cyber Crime*, Security Affairs, 26 July 2018. [Online]. Available: https://securityaffairs.co/wordpress/74764/malware/kronos-banking-trojan-variants.html.
[14] P. Paganini, "Underminer Exploit Kit spreading Bootkits and cryptocurrency miners," *Cyber Crime*, Security Affairs, 29 July 2018. [Online]. Available: https://securityaffairs.co/wordpress/74860/malware/underminer-exploit-kit.html.
[15] Tanya_K, "Source Code of Ratopak/Pegasus Spyware Targeting the Financial Sector Recently Leaked," Cyber Threat Insider Blog, 27 August 2018. [Online]. Available: https://blog.sensecy.com/2018/08/27/source-code-of-ratopak-pegasus-spyware-targeting-the-financial-sector-recently-leaked/.
[16] T. Hegel, J. Blasco and C. Doman, "Xwo - A Python-based bot scanner," AT&T Business, 02 April 2019. [Online]. Available: https://www.alienvault.com/blogs/labs-research/xwo-a-python-based-bot-scanner.
[17] Trend Micro Research, Europol's and European Cybercrime Centre (EC3), "Cyber-Telecom Crime Report 2019," Report, 2019. [Online]. Available: https://www.europol.europa.eu/publications-documents/cyber-telecom-crime-report-2019.