Geta MITREA[3]

Brian Krebs, *Națiunea spam. Din culisele criminalității informatice* [*Spam nation: The inside story of organized cybercrime*], translation from English by Dan Drumur, Bucharest, Romania, Preface by Eugen Glăvan, Corint Books Publisher, 2019

The book *Spam nation: The inside story of organized cybercrime* written by Brian Kerbs is translated from English by Dan Drumur and published at Corint Books Publisher in 2019. The original book is written in English and issued by the same author in 2014 under the title *Spam nation: The Inside Story of Organized Cybercrime – from Global Epidemic to Your Front Door* published in the United States by Sourcebook Inc.

As we can see from its own website https://krebsonsecurity.com the author worked as reporter on cybercrime during 1995 to 2009 at The Washington Post. And he was the author of more than 1,300 articles on Security Fix blog, washingtonpost.com and The Washington Post newspaper. As he mentions in his book the blog was a result after he decided to leave the newspaper and to write on its own about the cybercrime on the internet that affects all of us, including the younger generation.

Even though he is not a computer expert as he declares, in 1994 graduated with a Bachelor of Arts in International Studies from George Mason University and he documented by his own regarding the computer and internet security during his work as reporter and continuing after opening his own website. Meanwhile he published his book and participated in different presentations regarding cybercrime and elements connected to it.

Brian Krebs as reporter and author received different nominees and in 2013, together with security expert Bruce Schneier, was included in the Hall of Fame of authors of specialized blogs. In 2015 he won the Prose Award. His blog was voted three consecutive years (2011, 2012, 2013) by the RSA Conference, the biggest assembly on this domain, to be `*the blog that best represents the cybercrime security industry*`. The information presented on the blog is very well documented and has a proper presentation suitable for our current global and continuing adaptation to internet challenges for people. This can be considered a proper instrument for researchers, students, stakeholders that have their focus on cybersecurity and the spam issues that are all the time on the internet and even on our personal computers.

The book is structured on twelve chapters with and epilogue at the end, very useful for us as permanent current users of the internet. For the Romanian edition there is a preface written by Eugen Glăvan and a note regarding the

[3] PhD Lecturer, Department of Humanities and Social-Political Sciences, University Stefan cel Mare of Suceava, Romania; e-mail: mitrea.geta@gmail.com.

Romanian edition made by the Corint Books Publisher which refers to clarification of the translated word from English so that the reader would not mislead their interpretation. Also, in this edition there is included a glossary at the end of the book for helping the reader with specialized words in the domain.

We must mention that there is also included a section, at the beginning of the book, titled `WHO'S WHO IN THE CYBERWORLD` and contains data regarding the main names of the characters presented in the book who played a significant role in the cyber world during the different stages of evolution and events related in the book. There are fourteen characters from Russia or former states of the Soviet Union that are mentioned and for each of them there is a short description presenting their nickname known online and the cyber area that they act. For example, it is mentioned `*Pavel Vrublevski, a.k.a „RedEye"—Cofounder of ChronoPay, a high-risk card processor and payment service provider that was closely tied to the rogue antivirus industry*`. Similarly, are presented all the others famous characters from cyberspace.

Due to the fact that we also managed to access a part of the book`s version in English, until the publication of this paper, at the preface written by the author we are able to find his explanation regarding the usage of `spam` word in the title of the book. Because when all of us think about `spam` we associate it with the junk emails that we receive. And, sometimes we put it immediately in the trash or we access it and are able to infect our PS, laptop, phone, table etc. He mentions that from his point of view `*spam is the primary vehicle for most cybercrime*`, even though we are not aware of that and all of us, mostly the young generation, do not give it the importance that it may have on our electronic devices we constantly use.

In the first chapter entitled *Parasite* are reported methods used by cybercrime actors to send `spams` to our personal computers and ways that they remotely used `*to manipulate millions of PCs scattered around the globe into becoming spam-spewing zombies*` (Krebs, 2014:19). Even though, until now we did not perceive `spam` to be dangerous after reading this chapter we are able to find out that even once we had a `spam as parasite` in our PC and we did not even notice or take it into consideration. Maybe because of the fact that we probably didn't even know about the cyber world or because we trusted our antivirus producer and felt protected enough or maybe, as a young generation, we did not care enough and seem important to our daily life. We must take into consideration that people in specialized security institutions work to improve the antiviruses and create better firewalls to protect our system from this type of cyber attacks. But, we must not forget that `*the spam ecosystem is a constantly evolving technological and sociological crime machine that feeds on itself*` (Krebs, 2014:19). This is a permanent ping-pong between the actors involved in this system. Unfortunately, we are simply consumers and players due to the fact that we do not have the entire information and we are specialists on other domains.

Next chapters, titled `*Bulletproof*`, `*The Pharma Wars*`, `*Meet the Buyers*`, `*Russian Roulette*`, `*Partner(ka)s in (Dis)Organized Crime*`, `*Meet the Spammers*`,

`Old Friends, Bitter Enemies`, *`Meeting in Moscow`*, *`The Antis`*, *`Takedown`* and *`Endgame`* present ways that different hackers using trusted companies names with their server host in Russia managed to send `spams` to individuals from the network and used their computers as `zombies` to access personal information (birth date, phone number, bank account, life insurance details etc.) and collect them for selling online on black market sites for huge amounts of money. There are also presented the means they use for sending ad links to influence us to buy cheaper medication from an online market that confused us with similar names with the original ones. For example, buyers of Viagra pills want to keep their confidentiality and frequently use online websites to buy the medicine but they do not verify if it is original. And we do not have the means nor the security that corresponds with international or national reglementations and that is safe for our health.

We are able to find that people who bought medication via online websites listed their main reasons to be: lower price than the ones from usual pharmacies, accessibility, confidentiality, comfort, self-medication, recreation or addiction. As a portrait of these persons we may consider that they are single and the internet is their own information source. Some of them consider that they saved money and made a profitable business. Even though they risk their health due to the fact that they had now guarantee that those medications were real are possible to threaten their lives. As it happened to one consumer presented in the book.

Different types of cons are presented also, and ways that the specialists from cybercrime intervened *`complying with laws or regulations and preventing fraud or theft are the main reasons for investing in cyber security`* (Timofeyev and Dremova, 2022) and tried to prevent other similar situations. We must keep in mind that we can be without knowing users that can sustain online fraud or we can fight with this by updating our antiviruses and do not answer to unknown email addresses or links.

The author focuses on different types of attacks and mentions that:

> *`Ultimately, spam and all of its attendant ills will diminish very little without a more concerted, cooperative push from some of the richest and most powerful interests in the world, including the pharmaceutical industry; the credit card and banking sectors; lawmakers and law enforcers around the globe; and people like you and me, most of whom are the unsuspecting targets and victims of these spammers and hackers every day. It's time to do something about this global epidemic, to protect our identities, our bank accounts, our families, and our lives before it's too late`* (Krebs, 2014).

At the end of the book, we should focus our attention to *`Epilogue: A Spam-Free World: How You Can Protect Yourself from Cybercrime`* where the author presents solutions that we may use to protect ourselves from cybercrime. As possible solutions may be the usage of a secure password manager to keep all our passwords safe; as recommendations from the author are KeyPass, Saword Safe, Robo Form, LastPass. I believe that until present many more providers come on the

market and offer similar secure services, I must make sure they are trustworthy. Another solution is to use complex passwords from combinations of words, letters and special signs or even combinations of letters that do not form a known word from the dictionary. This strategy is used to make it difficult for hackers to obtain our information. We should download the apps from their official source and not from obscure websites. They use very similar names of the sites, so that we are misled and give them access to our data. And, the last possible solution to make frequent updates of the programs that we currently use. Because the owner includes new elements that fight against hackers.

In our global world and with permanent access to the internet we are exposed to new threats that we do not consider as dangerous as they are in reality. Even though the internet brought new useful features to our daily life, at the same time brought the spam or malware elements that put in danger our private lives and even our reliability. This book enlightens us regarding the dangers and risks that we are exposed to and offers us some possible solutions. All of us have the ability to `*guide the design of technical tools that improve the scientific community's ability to generate a safer and more secure cyber-environment*` (Maimon and Louderback, 2019) by adopting an informed online behavior and be aware of the permanent dangerous that we are exposed.

This book can be considered as a starting point for common internet consumers to help them to better understand the ways that internet and hackers can access our personal data and use it. The style used by the author is a friendly one and is easy to read even by inexperienced persons with IT specific terms. Personally, after reading this book I changed my online behavior and I am more cautious regarding what type of data I put online about myself or the type of passwords I used until now.

References

Maimon, D. & Louderback, E. R. (2019). Cyber, Dependent Crimes: An Interdisciplinary Review. *Annual Review of Criminology*, Vol. 2, 191-216, DOI: 10.1146/annurev-criminol-032317-092057.

Timofeyev, Y. & Dremova, O. (2022). Insurers' responses to cyber crime: Evidence from Russia. International Journal Of Law Crime And Justice, Vol. 68, DOI: 10.1016/j.ijlcj.2021.100520.

Krebs, B. (2019). Naţiunea spam. Din culisele criminalităţii informatice [Spam nation: The inside story of organized cybercrime], Translation from English by Dan Drumur. Preface by Eugen Glăvan. Corint Books Publisher, Bucharest.

Krebs, B. (2014). *Spam nation: The Inside Story of Organized Cybercrime – from Global Epidemic to Your Front Door*, Sourcebook Inc. Publisher, United States.