Journal of Forensic Research
ISSN: 2157-7145

Touzeau, J Forensic Res 2017, 8:6
DOI: 10.4172/2157-7145.1000401

Book Review Open Access

Behavioral Cybercriminals Differentiations between the Real World and the Virtual Space

Nadine Touzeau[1*]

Profiler, Net-Profiler-Behavioral and Environmental Analyst-Researcher, ACFE USA Member, Paris, France

[*]**Corresponding author**: Nadine Touzeau, Profiler, Net-Profiler-Behavioral and Environmental Analyst-Researcher, Paris France, Tel: 33641197673; E-mail: nt.profiler@gmail.com

Received date: November 16, 2017; **Accepted date**: November 22, 2017; **Published date**: November 27, 2017

Abstract

In order to thwart cyber-attacks, an antimalware program is set up or developed. That is to say, we learn cyber defense by considering that only viral intrusions are responsible for cyber-attacks. The human behind every cyber-attack is unfortunately obscured although human beings are the ones be find every cybercriminal act, they are the initiators whether in real or virtual space. In order to better understand this fact, the transversal universe and its occupants must be considered better than done nowadays. Investigating in virtual and real spaces is coming up against the very reasons that have created virtual space and that made cybercrime still growing strongly. In the virtual space, the occupants work differently to develop new behaviors; new ways of living and moving, even new ways of thinking that can sometimes be reproduced in the real space. In addition, the modus operandi circulates via the darkweb so that the lists can be reproduced and developed in the real space. The "original" signature changes according to the profiles that reshuffle offenses, which further complicates the investigations. Thus, integrating and understanding the cyber universe requires, above all, discovering new profiles in the cyber universe and making a behavioral differentiation between the virtual space and the real one according to specificities of the cyberspace itself. This is I am developing through the present research by exposing three concepts of mine: This is of “avatarisation”, “transverse zone” and “virtual intelligence.”

Keywords: Cybercriminals; Behavioral differentiation; Real and virtual World; Profiling; Avatarisation; Transverse zone; Virtual intelligence

Introduction

It is a fact, the human being has been overshadowed to curb cybercrime. In terms of defense, each attack suffered gives an answer by creating software, a machine, an antivirus, etc. But is this a machine that attacks your business? Is it software that steals your data? Is it an antivirus that is a scam to the President? Is YouTube that makes cyberbuyilling Of course not, because every action is committed by a human being? Integrating behavioral order to make predictive cyber security becomes a fact. However, the subject has been probably scratched due to a lack of knowledge of this universe, or even to recognition of it. Cybercriminal behavior in the cyber area is a part of behavioral sciences. Net-profiling is a profession more scientific and more cartesian than it seems. The body does not lie. Indeed, even behind the screen, your fingers on the keyboard, your posts, all information, move you to show us the elements and items that help us to build your profile. This is pushing my job in the virtual world where I can make lot discoveries about the hats behavior. In fact and according to some profiles, the hat does not have the same behavior in the virtual space with regard to the real one. Consequently, once making the behavioral differentiation, a part of the real can be reproduced. We should stress to the fact that this behavioral differentiation evolving, while cyberspace has not reached yet maturity, complicates the possibility of doing profiles from the virtual universe.

However, through my research work, I have developed some theories (since 2013) that helped me to build "generic" profiles according to types of cybercriminals where culture has a significant importance as well as education. It is believed too often that the cybercriminal has a mobile whether it is a gain, money fortune or something else. But this is not always true. All cyber-attacks are not often done by test or through gaming discoveries. Getting the best ranking, having a name, being famous by signing a big attack, being known but Medias as a genius in cyber intrusion are for the black hats an important driver to excel. Another element that should been integrated is that the fact that the cybercrime in the real world is offset by the crime in the virtual one, knowing that crimes, in the proper sense of the word, are rare. The 13th November terrorist attack in Paris is interesting crime case because it has been done using the Internet. Namely, some botnets intruded strategic firms as “Paris Airport” and “Orange operator”. It has been understood that it was for a robbery of some data but also, and why not, blocking some file to help terrorist in their actions as hiding a terrorist in his passage in an airport or blocking some important calls or emails etc. Criminal networks, trafficking of all kinds, work closely in the dark web and differently than in the real world. One obvious reason of this differentiation is the concept of “not moving”, “not being displayed publicly”, so “not proving” in a transverse area without frontier. Being behind a screen enables us more than what the real world can do. To allow the predictivity, by analyzing these behaviors requires other approaches than profiling which suits more the real world than the virtual one.

Discussion

According to the latest Euler Hermes study [1], 57% of French companies have been victims of cyber-attacks, knowing that few companies file a complaint when they are the object of a cyber-attack and that some of these cyber-attacks are not even revealed. According to this study, 53% of the causes are human. However, human beings are

not sufficiently taken into account in investigations, neither in defense organizations against cybercrime such as the ANSSI [2], nor in structures developing antimalware. Moreover, cyber-attacks are not only committed by malware or its equivalent, they may only be executed with humans, such as the fake President's scam developed by Gilbert Chikli [3]. Finally, whether clumsy or intentional, cyber-attacks are all committed by humans. The cyberspace's occupants have revealed, according to my studies and those of some psychologists such as Mary Aiken [4], what I call behavioral differentiations between the real and the virtual. In addition to the addiction to hacking developed by Djalila [5], probably the most famous behavioral differentiation, I will present some of my theories that I have developed and some of them are studying in French countries. When a company protects itself using cyber security methods, it sets up a dedicated service formed by the governance of technical engineers. Means are set up such as antimalware to secure the company. Thus, the company is supposed to be protected against cyber-attacks except that antimalware is designed after the detection of the computer virus to counter it. Indeed, cyber defense organizations cannot be predictive. However, the very nature of cybercriminals is that they do not reveal their crime or reveal it as late as possible, or even at a specific point in time. As a result, the hat is at least 1 to 2 lengths ahead. So why don't we understand first who these hats are? Their motivations? Why we can't stop them? Why do we take so long to apprehend them? Etc. If we learned to understand them, it would give us a head start, or even enables us to truly detect their crime. Indeed, could some cyber-attacks under cover of Ransom ware not hide a data theft? Companies' victims of cyber-attack, even if they pay the ransom and thus recover the data, have no guarantee that these data are not already on sale in the darknet. It is by learning how cyberspace works that I discovered that the occupants of this space develop different behaviors than those in real space. In other words, humans allow themselves to be different and live this difference in the virtual world. If we take the example of the young Tiziana Cantone, an Italian girl who was the victim of a sextape, namely a sexual video, which her companion published on the Internet without her consent, out of jealousy. The girl never stopped having this video removed, seen more than a million times. The press surfed through this story making fun of the girl. She ended her life. From what I understand, the press and his companion then apologized. They didn't know the harm it did to her, they didn't think their behavior could hurt her, simply because acts that are easy to perform in the virtual space, more satisfying than in the real world, once issued, are considered to be received just as virtually. In other words, the act being done virtually is considered to be received just as virtually without integrating the human being into the real world. Misunderstanding is at its height when cyber bullyers learn of the young woman's death [6]. However, by asking them whether they would have committed the same act in real space, they answer that they would not have done it. They do not allow themselves to behave in the real world as they do in the virtual one. It changes their personality. Is it duplicated? Is it more played in the virtual?

Conclusion

Many samples exist to show that cyber criminality has change in structural network. In results, it became very organized and more efficient. Neither antimalware, nor internet security professionals and organizations specialized in cyber defense have succeeded to stop the progression and growth of cybercrime. The way we fight against cybercriminals is the same as the one operated in real world, but hats surf on our failure in the real space. Our way of working, our laws, our mind, our

Spirit, the fact we take time to organize our think, to do our meetings, to group many points of view from colleagues, to make the best decision, this if made, are our enemies against fighting cyber criminality which lives and progresses with one click in a dark area. But the occupants of the virtual space are not machines, nor malwares or software, but absolutely humans: women and men who also live in the real space that is their world, their life. We can reveal their profile in the real world because they have developed some new behaviors. The fact they play with rules, what they could not do in the real world, develop their personality and profile that, sometimes they can reproduce them in the real world. Some of these hats have been recruited by you in your company, and sometimes they are persons with whom you drink a beer or play tennis, or even persons who take the bus with you each day. So near to you but not known by you as hats. Your own cyber behavior, the way you communicate in social network, the way you travel, all these elements gave many information to the cybercriminals about yourself (personality, weak). Net-profiling is the answer to find these hats and to reveal their target, to detect the trigger before they act, to understand their motivations. To be predictive in the face of cybercriminals who are two steps ahead of us. The predictivity will be our life buoy if we want to anticipate cyber-attacks. To be able to do it, we as scientists in different fields, we should study the human who is behind the screen, that human in cyberspace, the digitalized one with all his deviant behaviors in real and virtual spaces. We should also study his presence in this new area; the one where he feels good, his transverse zone and we should study also his way of living under create and live a new person by "avatarising" his true identity. The last but not least concept we should study is the virtual intelligent he develops gradually. Behavioral cybercriminal differentiations between real and virtual spaces using net-profiling, is a must as it proved its efficacy in many cases elucidated in a record time.

References

1. Hermes E (2017) French fraud study reveals rapidly increasing business cyber-crime threat. DFGC
2. National Agency for Information Systems Security, ANSSI.
3. https://fr.wikipedia.org/wiki/Gilbert_Chikli
4. http://www.maryaiken.com/cyber-effect/
5. Djalila RF (2017) The contribution of cyberpsychology and net-profiling to cybersecurity. El-Djazair.com.No. 110.
6. https://www.amazon.fr/NET-PROFILING-comportementale-cybercriminels-Nadine-TOUZEAUebook/dp/B018CFSZWO