

CYBER SECURITY – IS EVERYONE A TARGET?

Sozon A. LEVENTOPOULOS

(Security Analyst, CISSP, CASP, CEHv8, Security+, Network+)

Copyright: Research Institute for European and American Studies (www.rieas.gr)
Publication date: 8 August 2018

Note: The article reflects the opinion of the author and not necessarily the views of the Research Institute for European and American Studies (RIEAS).

It is a universal truth that today we live in the “era of information”. Like “stone”, “bronze”, and “iron” in the ancient years, “information” is what dominates our era. This “revolution” could not have taken place without the use of two technologies, the **Internet** and the **World Wide Web**. While easily confused these two technologies are vastly different¹. The combination of these technologies created the so-called “**cyber space**”. The “cyber space” is like a new universe, parallel and similar to our own. Unfortunately, it has and its “dark side”, the so-called “the dark web²”. It is where cyber-crime thrives and the main reason behind the creation of “**cyber-security**” a combination of protocols, best practices, tools and devices that are designed to maintain the CIA triad. CIA comes from the words **Confidentiality, Integrity and Availability**³ (and not the famous Intelligence Agency).

While “cyber-security” tends to deal with large-scale networks with the protection of extremely sensitive information or infrastructure it is a mistake to think that the average user, the one that connects to the internet mainly for recreational (like Facebook, Twitter, etc.) purposes and uses his computer, laptop or smartphone as an enhanced typewriter or camera it is not a **valuable target** for “cyber criminals”. On the other hand, the “average user” makes also the same mistake and his excuses like “I am not significant”, “I don’t have something to hide” are vastly common. Hidden behind these excuses, the “average user” will do nothing to protect himself and the computer system he owns, which in turn leads to the absence of security controls.

Here is why both are wrong.

“Cyber-crime” is a multi-billion “industry” that spans from industrial espionage to large-scale attacks to core infrastructures. Within the faint boundaries of “cyber-crime” we can also discover governmental agencies and state-driven actors that exploit both the absence of a firm law framework and the lack of forensic procedures and culture. In this framework, the “average user”

¹One could compare the Internet as the hardware and the WWW as the software of a computer system, but on a large planetary scale.

²The “dark web” is not a clearly defined area but it serves more as a term to include all of the “irregularities” of the normal – legitimate web.

³The explanation of every term of the CIA triad is not within the scope of its article.

is a valuable addition to the arsenal of a **hacker**⁴. The main reason why the “average user” is such an attractive target is mainly the lack of security culture and controls (like passwords, anti-malware programs, bad habits, etc.) which makes the duration of an attack very limited. Below we examine a number of cases:

Case No1. A hacker would like to disrupt the “availability” of a critical infrastructure. The easiest way to accomplish this is to “flood” that infrastructure with requests (the “ping of death” attack is the most common method). In order to do that he needs a large number of clients (or computers). The easiest way acquiring the necessary hardware is by “taking control” of someone else's computers and creating a so-called “zombie network” which will execute his command(s).

Case No2. A hacker would like to crack a password. It is well established that eventually every password or combination will be cracked. The goal is to span the required cracking time beyond a feasible threshold (usually mentioned in years). In order to diminish that time you need computing power which can be easily harvested from a “zombie network”.

Case No3. A hacker would like to access a well-secured computer system. The easiest way is to find the weakest link, which usually is an “average user” who fails to follow security protocols. The hacker could penetrate that user's personal computer, install a small programme that will infect the USB memory sticks connected to that computer and ultimately penetrate into said computer system from the inside⁵.

Additionally, a hacker could have access to bank information, social media passwords, tax records and to every bit of information, no matter how irrelevant or insignificant it may seem at first. It is worth mentioning that in the “dark web” you can find a variety of “zombie networks” (from a handful to hundreds of computer systems) to hire!

The main attacking vectors a hacker could exploit in order to hack such a computer system is luring or fooling an “average user” via e-mail, previously hacked web-pages or through pirated software or media. On the other hand, the first and the most important step an “average user” could take towards IT security is creating a “security culture” that balances between its knowledge, the sensitivity of information and usability he possesses.

Concluding, it is clear that “**Everyone is a target**”. Also, it is a universal axiom that you could never create a completely secure system (at least a usable one). In this article, the impact of an “average user” as the weakest link in the chain of cyber-security was examined by outlining why and how a hacker can and will attack the “average user”. Also, we should never forget that in the near future the security control will be extremely stretched and put into question with the implementation of “Internet of Everything” (IoE) which will interconnect every device on the planet (from computers to tablets, to microwaves, cars, etc.) and thus broadening the potential targets and attacking vectors. Until now we have not faced a full-scale cyber attack. Our dependence on information even in our everyday life makes the significance of cybersecurity even larger.

⁴Here the term hacker is used with its broader – unethical – definition.

⁵Actually this is how the STUXNET worm infected and ultimately crippled IRAN's nuclear program.