International Journal of Scientific & Engineering Research, Volume 8, Issue 1, January-2017
ISSN 2229-5518

Cyber Espionage and Digital Privacy

Magalhães R., Barbosa H.

Abstract— The act of cyber stealing your right of privacy as an individual is growing every day. Cyber Espionage is emerging along with the expansion of the World Wide Web, which origins a gigantic impact either on heavy solid economic, politic, agency groups, or on individual people. In this paper, we will explore some kinds of Cyber Attacks focused on citizens, and give a few hints in how you can protect yourself, in order to avoid your Digital Privacy to be violated, trying to making you much safer. How hackers can may not be the main threat for a common citizen is also described and defended along this paper.

Index Terms— Cyber Attack, Cyber Crime, Cyber Espionage, Cyber Protection, Digital Privacy, Technological Development, Spying.

1 Introduction

According to the World Wide Web, cyber espionage (also known as cyber spying) consists on the process/method of stealing secret information from the holder of it, without his permission [1].

Also, it's considered a cyber-crime, which stands for: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS[1]/MMS[2])" [2].

Mainly focusing on big targets such as governments, privacy industries and intelligence agencies, it's possible to split the hackers into two big groups: state hired hackers, in order to steal information from other agencies, and rebellions, who attempt to resell classified information or advanced properties, resulting on a possible huge impact on economy and terrorism. Can you imaine the impact of the stolen secret information?

Although, that's not it. You aren't safe. We aren't safe from the danger that the Internet leads us into. Being the target an indviual, hackers can track and trace a person's full life: knowing where he lives, where he usually goes, gain access to his credit card, everything. With the drastic raise of the technologies, we can see with our own eyes that we can access Internet everywhere we go. Day by day, more and more devices gain access to it, including Wi-Fi in restaurants, coffees, buildings, schools, hospitals, transports.

The more development we see, the more unsafe we are.

Along this paper, you will not only be able to see how does this kind of attacks work, especially those who can directly contribute to your right of individual privacy, but also how to avoid them protecting yourself. Focusing on the saying "hackers aren't the main threat of a common citizen", along this paper we will try to describe our point of view.

2 Technological Development

Technology improves every day. While this improvement continues, citizens all over the world will use more and more technological devices. Using more phones, computers and laptops [3] and with an undue protection [4], the chances of being spied on rise. The more technology grows, the more access a normal citizen gets. With this huge development, all over the world, people are almost forced to buy an improved technological device in order to adapt to the society. Formerly, a lot of misunderstood people will use non-protected devices. The risks of being spied on are high because most of the targets profiles are like this.

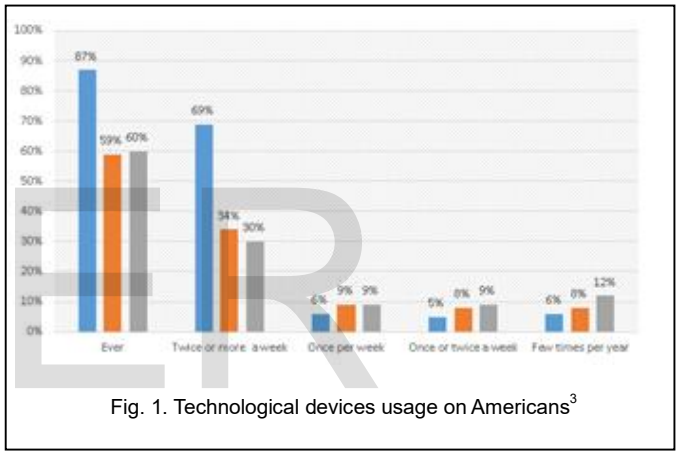

Fig. 1. Technological devices usage on Americans[3]

As you can see above, and now generalizing the America's population to the entire World, it's pretty obvious that the consumerism of technological devices is in a huge state of growth. Meanwhile, the risks of the violation of your privacy rights rise, directly proportional, considering an obvious statement that there is no system which provides 100% protection from being hacked (in this case, spied).

The main issue here is: are really hackers the biggest problem in order to defy your privacy rights? It is known by common sense that most of the hackers attempt to make a big move, challenging big companies' security system. According to Business Insider [5], these companies and groups are most in danger of getting hacked: sports teams, banks, celebrities and corporate espionage (companies).

So, if you, as a normal citizen, aren't really a main target of a hacker, what makes you think you are unsafe? Normally you would think you are "safe" now, but it's obvious that hackers aren't the main problem in normal citizens. This issue leads into another issue that will be developed below: What is the problem, then?

[1] Short Message Service
[2] Multimedia Messaging Service
[3] Image available on, https://www.cloudave.com/8235/2010-consumer-new-media-study-by-cone/

International Journal of Scientific & Engineering Research Volume
ISSN 2229-5518

3 Digital Privacy

Digital Privacy is "The right to privacy of users of digital media. Digital media raises such concerns for users as unpermitted use of personal information gathered from users' on-line activities and unpermitted release of that information to third parties." [6]

People expose themselves too much on the internet, that's common sense. As a quick example, look at all social networks such as Facebook, Instagram, Snapchat, were you can trace peoples' routines by looking at the number of pictures they post every day, describing everything they do, what they eat, what they wear, where they are. They do it innocently, without knowing the danger that is among them. Somehow, people still expose their children on the Internet, ignoring completely (or not having enough information) the dangers of it. But one thing is truth: nobody is safe. People can just try to find how to avoid some things. For example, we aren't 100% safe from a robbery in our house. How to make us safer? We lock the doors all night, we install home alarms and security systems.

So, how this works among the cyber space? On the next chapter, we will explain how a citizen's digital privacy can be violated by giving some examples.

4 Cyber Espionage

To attack and to defend yourself from being spied on. There are many kinds of ways to spy on you, some of them are just conspiracy theories. Meanwhile, there are a few known examples of Cyber Espionage attacks that we will try to explain later on this paper. In order to start our explanation by giving some examples, we will start telling you what is the Five Eyes Alliance.

4.1 The Five Eyes Alliance

Historians trace the origin of the Five Eyes Alliance to the World War II era, when American and British intelligence collaborated closely. After the WWII, USA and United Kingdom decided to keep sharing intelligent data with each other. Although, not only USA and UK this time, but also Australia, Canada and New Zealand. Meanwhile, they established an agreement that enabled them to share all kinds of secret surveillance intelligence with each other. Their joint operations were explicitly related to "foreign intelligence", which is the agreement defined as "all communications of the government or of any military, air or naval force; faction, party, department, agency, or bureau of a foreign country; or of any person or persons acting on purporting to act therefor, and shall include communications of a foreign country which may contain information of military, political or economic value." Not surprisingly, most of the information shared between USA and UK intelligence agencies pertained to the Soviet Union and other Cold War foes in Eastern Europe and Asia. [6] [7]

Fig. 2. The Five Eyes Alliance in a World Map[4]

4.2 Attacks on Citizens

On this chapter, we will give two examples of two different kind of attacks on citizens, by violating their privacy rights, in order to spy and collect info (control) of an individual.

The 5 American-Muslim Espionage, after 9/11[5] many changes happened on the USA's national security policy objectives due the lack of preparation to avoid it. "Perhaps, no administration could have prepared the American public for such a radical attack that so few anticipated." The consensus after the tragedy was that intelligence security systems had to be strengthened so another attack like this would never happen again. [8]

Since the attack was led by Al-Qaeda[6], which is a Muslim organization, USA decided to keep an eye on the American Muslims inside the USA. According to some leaked documents by a former NSA contractor, it's now proved that the NSA have been spying on Muslim's citizens, which can lead to legal standing against a possible sue to the government.

The targets of this spying program were 5 American-Muslim citizens who completely deny any kind of involvement in terrorism or espionage. These targets include an "advisor for the Bush administration's Department of Homeland Security; a civil rights activist, who was formerly a political science professor; an executive director of the Council on American-Islamic relations; a lawyer who has represented clients in cases connected to terrorism; a professor at a University."

Listing 7,485 email addresses, 202 of them belong to Americans, while the others nationality remains "unknown". This controversial document called FISA[7] lead to strong debates between the US government and Foreign Intelligence Surveillance Court, where Americans tried to explain and defend that their belief was that some Americans are agents of terrorist organizations and may be helping actively on terrorism and espionage attacks.

"The Department of Justice and the Office of the Director of National Intelligence strongly deny that the US monitors activists simply because of their race, religion, or dissenting views."

Even still, they don't deny that they put in practice these kinds of situations every day, illegally spying on citizens like were referred above.

[4]Image available on, https://en.wikipedia.org/wiki/Five_Eyes
[5] 9/11 – 11th September, 2001, one of the most horrible terrorist attacks.
[6] Al-Qaeda – Terrorist Muslim organization responsible for the 9/11's attack.
[7] FISA – Foreign Intelligence Surveillance Act.

International Journal of Scientific & Engineering Research Volume ŁŁÛu(ÚÚÜÌuhuÛu)ÈÒÜÈÙà ı l Ɣhƛuu
ISSN 2229-5518

To conclude this example, it's still not clear why these citizens were spied on. The only logical answer was due to their race, religion and cultural background. Is that ethic? Doesn't it violate their own privacy rights? How can you be judged by your color, your race, your religion? There are many issues unsolved, but even still, after the 9/11, the security system was forced to develop. Unfortunately, situations like this keep happening. [9][10]

Is the 9/11 attack a justification to the constant violation of the privacy rights within the citizens? Can it be used as an excuse to spy all citizens?

Google Voice, searching in Google something is growing every second. There are 3.5 billion searches per day and 1.2 trillion searches per year worldwide. [13]

After a little research, ironically on Google, we found that it's available to search using your microphone instead of your keyboard with a new feature called Google Voice.

As you can see below, we tried it ourselves and look the results. Google is linked with your microphone in order to provide another way to search on the biggest search engine on the Internet.

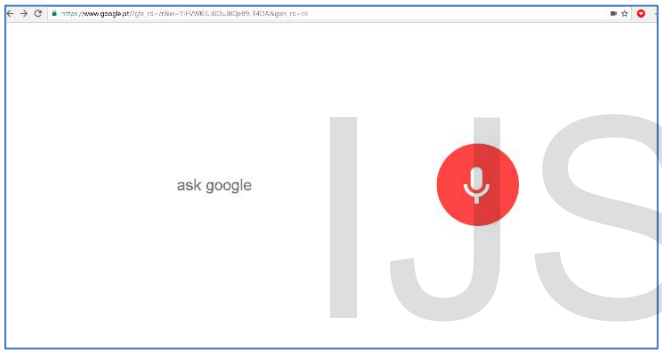

Fig. 3. Google Voice, ask google

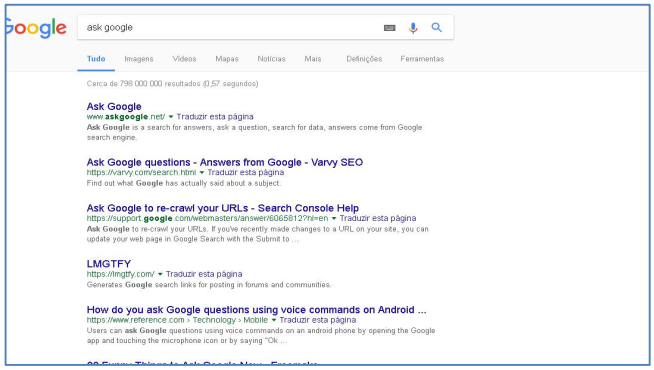

Fig. 4. Ask google, search

Until here, everything seems great. But we also found that everything we search on Google is stored on "My Activity", which is a page linked to every Google account.

Google claims that only the owner of the account can see his history, that Google protects his privacy and safety.

One thing is certain: all research is stored, including our voices. Meanwhile, Google can easily track our activity, what we like, what we search most. With it it's possible to almost track a person instantly. Not only the audio recording your voice, but also the way that all data used can be easily accessed by Google as we referred in the first example of Muslim-Americans which had their e-mails checked.

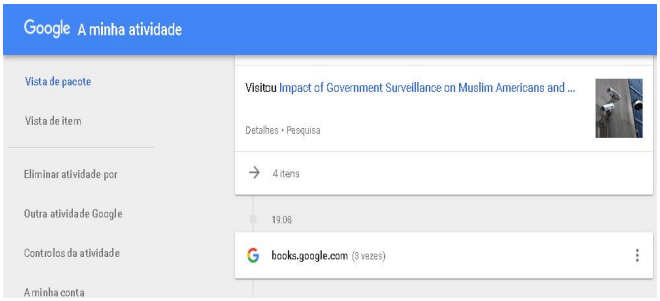

Fig. 5. Google My Activity

But how to avoid this kind of things? Well since you are aware of this Google Voice, you are also aware of many examples such as Xbox and Televisions who also listen to you. [12]

Being just a threat, with this example you are already warned about this Google feature. It is your choice if you want to use it or not. Besides, everyone uses a social network, where similar data is stored which can have pretty much the same result.

To finish this example, we would like to bring back our main objective for this paper which is to try to explain why hackers aren't the main problem for common citizens but the big companies who have access to lots of data and can easily track every single thing in our lives.

4.3 How to Protect from Cyber Attacks

After a little research and trying to generalize this part of the paper, we tried to check the amount of protection that a person can get in order to avoid many kinds of companies/hackers' attack.

First of all, we should assume that technological improvement also results in an improvement of hackers and companies' knowledge. As they get more sophisticated, penetrating companies firewalls in order to access data from a customer will happen. Although, companies are also implement strong securities system.

If you are a costumer, how can you avoid some data breach in a company you are signed in?

For example, if you want to protect yourself as much as possible if you are signed in a bank, you will have to check every week if there's an anomaly on your credit card statements. If anything looks suspicious, you can report it to the bank as soon as possible. Many bank have programs on real time which warns the customers if anything suspicious is happening on their accounts, for example, trying to make a payment which passes the daily/weekly limit that you implemented on it, the bank will instantly contact you via SMS, phone call or email.

There is also a constant threat to your personal data. Take precautions on giving information to random people, to advertisement callers, try to login on sites which the web address begins

International Journal of Scientific & Engineering Research Volume
ISSN 2229-5518

with "https" [8]

You can also try to change your passwords every once in a while, trying to avoid your initials, your date of birth, your surname, etc. Simple passwords can result to an easy hack due to the simplicity of them. [14]

Try to use different passwords for every website, using different id and password combination; activate your firewall and make sure you have a good anti-virus. Don't install cracked software, avoid suspicious links, never upload unencrypted personal data online, try to ignore random advertisements and suspicious emails. [15]

5 Conclusion

As the world is, with a huge technological development, it's certain that the risks of being Cyber Attack raise as well. After you connect to the Internet, you lose your 100% safety. Your Digital Privacy might be violated and we tried to describe how that could happen by giving two examples (one real history example and one we tried for ourselves).

How hackers aren't the worst problem for common citizens? We believe and explained our points, by referring two examples in how big companies can be a bigger threat than a random hacker.

Talking about American-Muslims, we tried to justify the unjustifiable spies, giving the after 9/11 reason which can be used as an excuse right now in order to spy who they want to.

By giving our personal Google Voice example, we tried to defend that some new featured apps, add-ons, aren't that amusing as they look. In little things, they can store our data, save our voice, track our entire life.

Since it's important to try to preserve your privacy as much you can, we also tried to give some hints about some things you should avoid, so you could be a little safer with these little things you can do.

By searching more, you collect more info, and you also can protect yourself even more, because like we defend, you are never safe.

References

[1] Cyber Spying, Techopedia, https://www.techopedia.com/definition/27101/cyberspying, 2016.

[2] D. Halder, K. Jaishankar, "Cyber Crime and the victimization of women: laws, rights and regulations", 2011.

[3] Wang Y., "More People Have Cell Phones Than Toilets", Time Current & Breaking News | National & World Updates, http://newsfeed.time.com/2013/03/25/more-people-have-cell-phones-than-toilets-u-n-study-shows/, 2013.

[4] Siciliano R., "More Than 30% of People Don't Password Protect Their Mobile Devices", Mcfee https://securingtomorrow.mcafee.com/consumer/identity-protection/unprotected-mobile-devices/, 2016.

[5] Cook J., "Business Insider, meet the biggest targets for hackers", http://www.businessinsider.com/the-biggest-targets-for-hackers-2015-3, 2015.

[6] Dixon P., "Surveillance in America: An Encyclopedia of History, Politics, and the Law", 2016.

[7] Howe F. G., "The Early History of NSA", https://www.nsa.gov/news-features/declassified-documents/cryptologic-spectrum/assets/files/early_history_nsa.pdf, 2007.

[8] Bolton M. K., "U.S National Security and Foreign Policymaking After 9/11: Present at the Re-creation", 2008.

[9] McCormick R., "NSA and FBI spied on innocent Americans after 9/11 because of their race and religion", http://www.theverge.com/2014/7/9/5835772/snowden-leak-confirms-us-spied-on-american-muslims, 2014.

[10] Greenwald G., Hussain M., The Intercept, "Meet the Muslim-American leaders the FBI and NSA have been spying on", 2016.

[11] Louv J., "Google Chrome's New Feature: Spying On You for Google", http://ultraculture.org/blog/2015/02/13/google-chromes-new-feature-spying-google/, 2015.

[12] Falkvinge R., "So Google Records All The Microphone Audio All The Time, After All?", https://www.privateinternetaccess.com/blog/2015/10/so-google-records-all-the-microphone-audio-all-the-time-after-all/, 2015.

[13] Internet Live Stats, http://www.internetlivestats.com/google-search-statistics/, 2016.

[14] Lopez P.," 5 Ways To Protect Yourself From Cyber Attacks", http://www.forbes.com/sites/realspin/2014/02/07/5-ways-to-protect-yourself-from-cyber-attacks/#4dd726a959a3, 2014.

[15] Barot A.,"How to protect yourself against cyber-attacks", http://cyberworldmirror.com/cyber-security-15-simple-steps-to-protect-your-self-against-cyber-attacks/, 2015.

[8] HTTPS – Secure Web Site