A Review on Cyber Attacks and its Preventive Measures

Pedro Teixeira

Lusofona University of Porto, Portugal
pedroalv_23@hotmail.com

Abstract. The aim of this paper is to be able to approach the questions of privacy and security on a review about cybernetic attacks and its preventive measures. It will be discussed the impact of these attacks on modern society and how they change the way of how we need to view things in order to improve the way we work, play and entertain ourselves. This paper will also include a study of the potential attack we can suffer and the explanation of why it is one of the most dangerous in my opinion. It will also show the capabilities of the attack and how we can try to prevent the attack.

Keywords: Inside Job, Social Engineering, Blackmail, Ransomware, WannaCry, Encryption.

1 Introduction

In today's standards Cybercrime is a well-structured business in which big teams made of highly trained hackers make a profit by just attacking vulnerable companies or even common individuals when they are exposed to these hackers by not taking the necessary measures to prevent the attacks. [1]

As the years progress not only does the technology advance, but the criminal environment in the cybernetic world also does, which means that almost everything is connected to the internet in some way or another, meaning, that the number of doors from where hackers can attack is endless. Starting with simple pranksters joking on the internet sending some spam into mail-boxes, to professionally organized people attacking bank accounts and breaching into big companies to able to steal their personal data, therefore we live in a world where cyber threats and attacks are recognized as political and commercial challenges with levels of financial and reputational consequences. [2]

Knowing all this, we need to stay up to date in every way possible in order to keep up with what we can be struck with, so it is more than important to know what cyber-attacks are, how to spot a potential one and protect ourselves. [3]

The first section of this paper is going to explain how we can describe a cyber attack as well as the common scenarios that they occur on, thereafter, preventive measures will be detailed so we can have a better understanding how on to avoid certain risks.

In section three we are going to look at the current situation about cyber-crime around the world and a brief topic on how things are developing in Portugal.

Lastly, in the final section of this research paper, an exposition about one of the potential attacks based on encryption will be explained as well as detailing how we can prevent getting infected and how to proceed if we were already attacked by the virus.

2 Cyber Attacks

A cyber-attack is generally known by the common user as someone trying to steal our information or compromising our own device. Attacks can vary in terms of goals, one can be aimed to disable or turn offline a desired computer or electronic device, another goal is to gain access to said computer or electronic device and steal its data and gain admin privileges on it. [4]

As said before, cyber-attacks can have behind them a diverse spectrum of intentions, attacks on the general public or corporate organization can be or will be carried out through the spread of malicious viruses, fake websites, denial of services etc. The amount of ways today on how we can breach security for personal gain is enormous. [24]

2.1 Common Cyber Attack Scenarios

In terms of organizational attacks, we can trail a vast number of scenarios where they can occur.

Inside jobs are one of the most common ways of attacking a company or organization, most of the time when your company gets attacked, that threat is coming from the inside, where an employee working at said organization may exploit his role in the company to have access to confidential information by hacking the computer's network that is available to him. One of the most dangerous aspects of inside jobs is that the access to these personal information's are coming from trusted systems, and because of this most of these threats will pass undetected mostly because the attacker can erase the evidence since he has all the control.

The 2017 Cyber Security Intelligence Index by IBM concluded that 60% of the attacks organized against corporations were made by insiders, the aim of these attacks mostly involved malicious intent. [5]

Social Engineering is considered the technique used by attackers to lure users into sending them their confidential data. Social Engineers take advantage of human behavior to accomplish their illegal goals, one of the methods to capture the personal data of the victims is either by impersonating, for example, an IT support employee and trick the victim into divulging passwords and confidential data or simply by using the method of "phishing", were the victim opens a link to a fake website where they are prompted to insert their personal information, what they don't realize is that the website where the data is being inputted is fake and the information is, therefore, going directly into the hacker's hands. [5][6]

Blackmailing and extortion have been around for a long time, it has been used long before the internet was even a "thing", for ages now people around the world try to gain advantages in

terms of money, property, promotions or simple revenge with the use of blackmailing another person by threatening to expose private information. [5]

Nowadays it is even more common these types of crimes because a hacker can for have to access private pictures of someone and then ask them for money, so they won't expose the photos. Everyone now has a phone that is connected to the internet making it relatively easy for some expert to gain access to it, the sheer amount of cases of blackmail and extortion around the world is exponentially higher each year, Fig.1 shows the statistics of the number of recorded offenses in England and Wales from 2002/03 to 2017/18. [5][7]

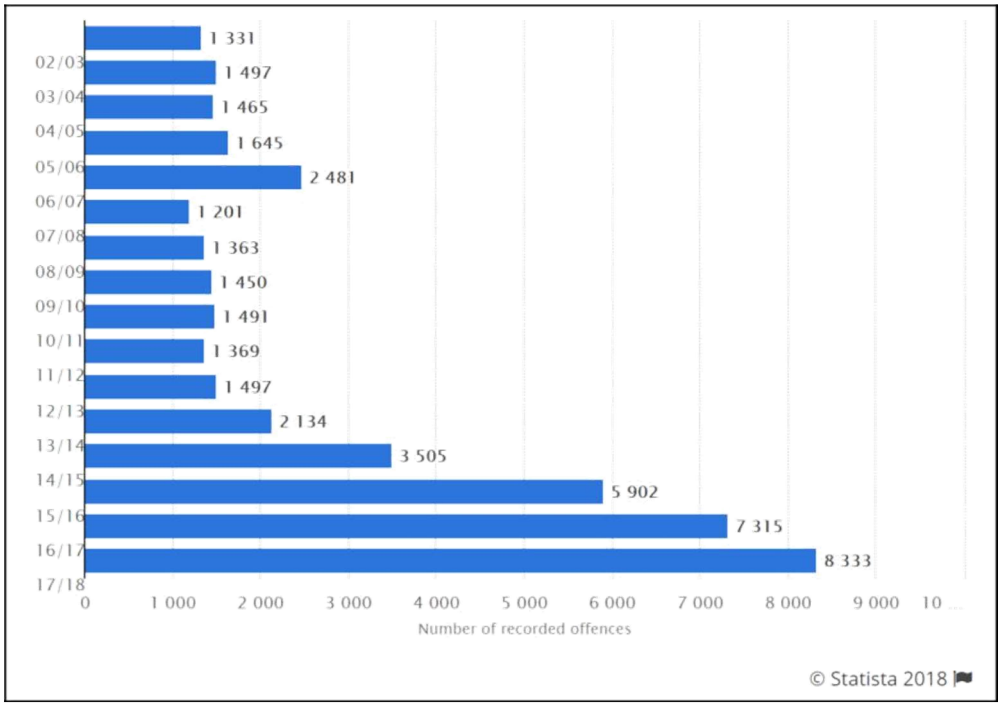

Fig.1. England and Wales Offences Recorded

2.2 Common Cyber Attack Preventive Measures

According to multiple articles, 2017 was a year where many companies suffered from security breaches and largely because of the lack of preventive measures. 2018 on the other hand, is proving to be a year where most of these companies are investing more and more money on security, this said we can follow some of the steps to prevent some of the described examples of cyber-attacks:

- Inside jobs

To try and prevent these types of attacks we can conduct background checks before proceeding to employ any candidate to the company, doing a review on the criminal, financial and commercial background will only benefit the company by making sure the employee is always telling the truth, since there is also an estimate that 40% of resumes might contain false information, so making sure we are employing the right person is crucial to prevent an inside job. [8][9]

Other common ways to prevent this issue is by having more than one trusted person overseeing the financial system of the company as well as restricting the number of employees who have access to back-end information, this way we can create an efficient and controlled environment of the crucial information the company has, preventing the risk of an inside job. [8][9]

- Social Engineering

According to most opinions the best way to combat social engineering is no more than educating yourself against these threats, you cannot protect yourself if you don't know where the threat is coming nor how the threat is coming, so it is essential for oneself to study and understand how threats are conducted so we can have a bigger understanding on the precautions to take and possible educate others into not making the mistakes that can lead to a possible act of social engineering. [10]

These types of attacks are also common and dangerous are in video game clients, where people can impersonate admins by asking passwords of un-educated and naïve young gamers, these people will often ask for personal information in order to steal either the account itself that has value money wise thanks to the games that the account contains or credit card information. Yet again, educating oneself and being aware of messages like the ones in Fig.2 and Fig.3 where there will always be a message saying that no admin will ever ask for your password of personal information. [10]

Common sense in general is the biggest weapon, being aware of the dangers and always suspect of the most obvious questions and simple forms on the internet, always checking if the website we are navigating on has the SSL (Secure Socket Layer) enabled, so we know there is no danger in clicking or providing our information. [10]

- Extortion and Blackmail

Extortion and blackmail are always a sensitive theme to describe since most of these attacks are often about intimidating us directly through threats and money in exchange of deleting any private information, they allegedly have acquired from using viruses. To be clear most of these threats normally are fake and only exist to intimidate us into giving the culprit money in form of a bitcoin, so when we normally receive an e-mail like the one in Fig.2, we should just ignore it, or simply never open an e-mail from an unknown source before checking it with an antivirus, this is just a scam so we should remain calm and collective the sender did not install anything on our computer nor did he use a keylogger to get access to our credential and private photos and videos of us. [11]

GMX - (Part num your Hacked phone. +XX XXXXXX0837) Seite 1 von 1

GMX ProMail

(Part num your Hacked phone. +XX XXXXXX0837)

Von: [redacted]
An: [redacted]
Datum: 10.08.2018 17:00:12

It seems that, +XX XXXXXX0837, is your phone. You may not know me and you are probably wondering why you are getting this e mail, right?

actually, I setup a malware on the adult vids (porno) web-site and guess what, you visited this site to have fun (you know what I mean). While you were watching videos, your internet browser started out functioning as a RDP (Remote Desktop) having a keylogger which gave me accessibility to your screen and web cam. after that, my software program obtained all of your contacts from your Messenger, FB, as well as email.

What did I do?

I backuped phone. All photo, video and contacts.
I created a double-screen video. 1st part shows the video you were watching (you've got a good taste haha . . .), and 2nd part shows the recording of your web cam.

exactly what should you do?

Well, in my opinion, $1000 is a fair price for our little secret. You'll make the payment by Bitcoin (if you do not know this, search "how to buy bitcoin" in Google).

BTC Address:

1GYNGZLEUGkkQjHo19dHDnGE87WsAiGLLB

(It is cAsE sensitive, so copy and paste it)

Important:
You have 48 hour in order to make the payment. (I've a unique pixel in this e mail, and at this moment I know that you have read through this email message). If I do not get the BitCoins, I will certainly send out your video recording to all of your contacts including relatives, coworkers, and so on. Having said that, if I receive the payment, I'll destroy the video immidiately. If you need evidence, reply with "Yes!" and I will certainly send out your video recording to your 6 contacts. It is a non-negotiable offer, that being said don't waste my personal time and yours by responding to this message.

Fig.2. E-mail sent by the attacker [11]

Nonetheless we should change our passwords regardless if we get these types of e-mails or not, a good practice is changing the passwords often and not having the same password for different types of platforms, but more importantly, than that is having a two-step verification in order to diminish the risk even more. [11]

A powerful and easy tool to use to see if our credentials have been leaked or stolen, we should use this website called ‘https://haveibeenpwned.com/’, this useful tool will actually tell us which platform had the credentials leaks and a Pastebin with a conjunction of thousands of other e-mails that have also been affected. [11]

Fig.3. "Have I been PWNED" results [25]

When we type our e-mail, it will show us the number of breaches our account has suffered has shown on Fig.3, in this example a game, a video sharing platform, and some other data breaches from other websites our e-mail was registered in. This tool is very handy has it also shows the actual data that was compromised and released to the public as well as the year that it occurred.

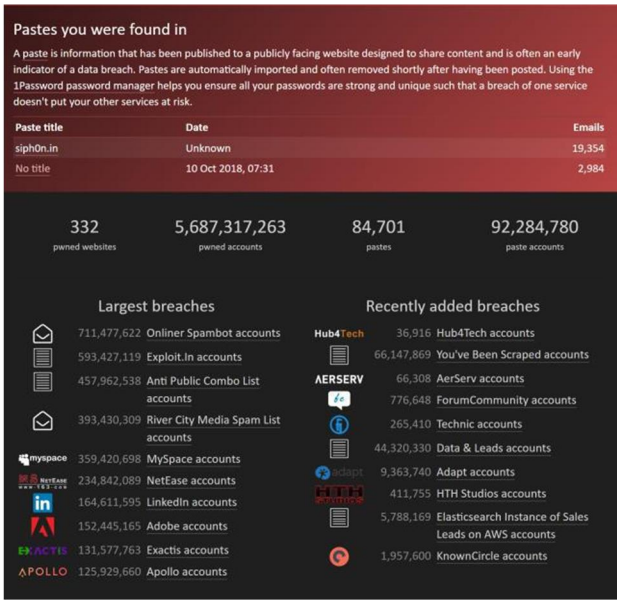

Fig.4. "Have I been PWNED" Results [25]

Fig. 4 shows us the Pastebin that can be consulted, there we can see the actual e-mail that was stolen and released to the public alongside ours, below that we have some stats of the websites that were breached, the number of 'pwned' accounts the numbers of pastes and paste accounts. Even so, we can see some highly regarded websites like Adobe and LinkedIn were also attacked.

3 Brief Overview of Cybercrime Around the World

Cybercrime is a non-stop topic around the world, global cybercrime costs are estimated to grow annually and will reach a historical number of 6 trillion dollars by 2021 compares to its half counterpart of 3 trillion dollars in 2015 [12]. These numbers consequently projections based on historical cybercrime figures, these costs will include the destruction of data, stolen money, theft of personal and financial data, fraud and many other vulnerable types of data. [13]

Converging all these topics around attacks and threats the United Nations specialized agency for information and communication technologies measured that countries around the world are committed to preventing and improving their priorities around this matter, even though less developed countries like African regions still lack the means necessary to combat these threats remain mostly dependent of other countries support. The main areas being the focus today are:

- Safeguarding digital business models
- Utilizing Intel and info-sharing programs
- Security of the Internet of Things
- Managing geopolitical cyberthreats

Reports from multinational professional services firms believe based on surveys conducted to CIOs and CISOs concluded that organizations appear to be moving in the right direction in terms of adapting to the current situation of attacks, meaning they can now prevent and foresee these threats resulting in a recovery time that may vary between minutes and within a certain amount of hours for 44% of the companies. [13] [14]

Ransomware, banking malware and mobile malware continues to be the most significant threat at this moment in time because to date there is no system immune to the infection. [13] [14]

3.1 A Brief Look at Portugal

As shown cybercrime grows exponentially each year, and stats show how well and how much countries around the world are evolving to prevent the attacks and actually help others with these problems, therefore in 2016 a unit focused on cybercrime and cyberterrorism was created in Portugal the law was approved and enabled the National Police to have this unit based on a model adopted by EC3 (European Cybercrime Center) from EUROPOL. Thanks to this unit Portugal can and will be able to respond in a fast and efficient way to cybercrime. [15]

However, creating this unit will not solve all the problems since according to APAV (Associação Portuguesa de Apoio à vítima) estimated that 78% of people in Portugal that surf the web are not well informed about the risks and threats. [16]

Attorney Pedro Verdelho alerts that cybercrime has gone up, which is a fact and common occurrence around the globe, but on the other hand, there are not credible statistics about it. The attorney states that no one in Europe has such rigorous numbers, this is due to the stats not being covered in the right way, meaning that the crimes are being recorded yes, but not how the actual crime was convicted, the same way a crime occurs but we don't have a record if the crime was online or not. [17]

Cybercrime fighting unit from the National Police responsible Carlos Cabreiro, admits also that cybercrime is going up stating extortion and identity theft being the one that is growing the most. Exposing our personal data on the internet is the catalyst for this growth since gathering all our details is easy which leads to fake accounts on social media and impersonation for all other kinds of activities. [18]

4 Ransomware

Ransomware is one of the various types of malware that exists today, these true purposes of these viruses is to block the access to computers and mobile devices or encrypting the data existing in a system, usually, the attacker demands money for the restoration of the device and/or data that he managed to gain access to. [19]

Many times, the logo of INTERPOL or a law enforcement agency is displayed to the victim making them believe the authorities are involved in any activity, even though this is not the case because INTERPOL or any other agency will ever block or encrypt data of any user. [19]

4.1 "WannaCry" – The Attack

WannaCrypt also known as WannaCry on May 12th of 2017 started spreading along multimer networks infecting thousands of computers across the globe, 24 hours after the first attack the actual number of infections reached a number as high as 185.000 machines in over 100 countries. [20]

This attack was aimed at mostly hospitals, telecommunication companies, and gas plants. One of the companies that were damaged the most was the National Health Service (NHS) located in the United Kingdom. [20]

Ransomware is normally used to infect small to large businesses across the world making its way to systems and networks via attachments on e-mails, browsers or third-party exploits, ransomware like WannaCry automated the exploitation of a vulnerability present in most versions of Windows. This potent Ransomware is one of the most dangerous nowadays thanks to the ability that allows the attacker to run code on the vulnerable computer enabling him to plant ransomware without human and local action. This behavior of an attack was never seen

before allowing it to be the perfect attack against specific environments or infrastructures like servers running vulnerable versions of the Server Message Block (SMB protocol). [19] [20]

The attacker solicited a rescue of 275€ to 550€ which makes it believe that the attackers aimed at smaller businesses, so they amassed attacks based in quantity and not in quality. [21]

4.2 Preventing WannaCry

The correct way to prevent them from being affected by WannaCry is using a a copy of Microsoft Windows that is not up to date:

- Windows 10 (1507,1511,1607)
- Windows 8/8.1
- Windows 7
- Windows Vista
- Windows XP
- Windows Server 2008, 2008 R2, 2012, 2012 R2

Therefore, the first step into prevention is always to keep the device up to date with all security patches installed. [22]

But what if your machine is already affected?

Fig.5. "WannaCry" Infected Warning

As shown in Fig.5 this is what will appear if your computer is already infected with the ransomware, you will be prompted with a countdown that tells us that, if we don't pay the demanding money, our files will get deleted.

There is no current fix for the virus if one's computer is already infected even though experts are working towards finding ways to decrypt the files. The advice that should be taken is reformatting the computer, restoring a previous version or installing a new version of windows and restoring the data files that have been backed up. Although in recent months project "No More Ransom" is being developed by the National High-Tech Crime Unit of the Netherlands police, Europol's European Cybercrime Centre and McAfee. [19] [22] [23]

In no way or form should we ever adhere to their demands for the money they ask as reported by The Guardian via Europol. [22]

In general, we can be avoiding ransomware by updating and installing software and security patches, this is key to avoid infection as well as never jailbreaking or rooting any device. [22]

5 Conclusion

Human behavior is and will keep being the reason why most crimes happen, taking advantage of one's ingenuity or lack of knowledge on the subject, will result in someone exploiting a service, blackmail someone, extort another or steal their identity. The trend for cybercrime is to actually keep increasing as well as the diversity of the threats we may face in a near future, ransomware like WannaCry that surged in a way no one was expecting, creating such an impact that even today experts don't have an official way of preventing or recuperating the encrypted data, are signs that these methods of exploitation will keep evolving and developing, we can come to terms that if someone wants to break in they will, it is just a matter of time and resources until someone breaches whatever their target is.

Spreading the word as much as possible to keep preventing and minimize damage is crucial. Reducing the number of violations of privacy and theft must be a priority, seeing the numbers and statistics means that if nothing is done, more and more crimes will be committed.

Nonetheless, not everything is bad, as we can clearly see giants like INTERPOL and EUROPOL keep moving masses and creating ways to give tools to start preventing most of the crimes as well as national police in Portugal being allowed to have a unit to combat these threats and be able to respond faster and more efficiently.

Taking in consideration most of the aspects reviewed in this research we can conclude that the wave of crime is indeed increasing at a steady rate either by the creation of new exploits, taking advantage of misinformed people, poorly configured systems, outdated software and the most common of all human behavior in which leads to other types of threats like extortions and blackmailing, we can also rest assured that the big companies and associations worldwide are aware of this problem and are creating ways and the means necessary to swim against this current that seems too heavy to be taken care of. Countermeasures must evolve as fast, if not faster than exploits, no one wants to be in the bitter end of the deal, so its everyone's duty to

make the cyberspace a cleaner and healthier place, overall every single individual is responsible for alerting and contribute to better environment online and offline.

References

1. "Anatomy of a Cyber Attack the Lifecycle of a Security Breach", Oracle Linux, Retrieved from: "http://www.oracle.com/us/technologies/linux/anatomy-of-cyber-attacks-wp-4124673.pdf", Last Access: 20 December 2018.
2. "The Evolution of Cyber Attacks", ITBusinessEdge, Venafi (2013) Retrieved from: "https://www.itbusinessedge.com/slideshows/the-evolution-of-cyber-attacks.html", Last Access: 20 December 2018.
3. Ledford, J.; "Could a Cyber Attack Knock Out Your Computer?", Lifewire (2018).
4. Fruhlinger, J.; "What is a Cyber Attack Recent examples show disturbing trends", CSO from IDG (2018).
5. Farhat, V.; McCarthy, B.; Raysman, R.; "Cyber Attacks: Prevention and Proactive Responses", Holland & Knight LLP, Practical Law Company (2011).
6. Hulme, G.; Goodchild, J.; "What is Social Engineering? How criminals take advantage of human behavior", CSO from IDG (2017).
7. "The Crimes of Blackmail and Extortion", Law Shelf Educational Media, A project of National Paregal College, Retrieved from: "https://lawshelf.com/videos/entry/the-crimes-of-blackmail-and-extortion ", Last Access: 20 December 2018.
8. Doyle, A.; "What Employers Look for in Background and Credit Checks", Background Checks for Employment, the balance careers (2018).
9. Mueller, K.; "Deter the Inside Job. 5 Ways to Avert Employee Theft and Fraud.", Entrepreneur Europe (2018).
10. Olavsrud, T.; "9 Best Defenses Against Social Engineering Attacks", eSecurity Planet (2010).
11. Jareth.; "How to deal with cyber blackmail?", EMISOFT, Security Essentials (2018).
12. Periman, K.; "How to Prevent the Bank Robbery No One Can See", 2017 Midyear Cybersecurity, Report Cisco Blogs, Financial Services (2017).
13. Steve, M.; "2017 Cybercrime Report", Cybersecurity Ventures, Herjavec Group (2017).
14. "2017 Global Enterprise Security Survey", Fortinet (NASDAQ: FTNT) (2017).
15. EC3Europol.; 2015, 7 October 2016.; Retrieved from: "https://twitter.com/EC3Europol", Last Accessed: 18 December 2018.
16. "A Realidade do Cibercrime", APAV, Retrieved from: "http://apav.pt/cibercrime/ ", Last Access: 20 December 2018.
17. Verdelho, P.; No stats from cybercrimes, Retrieved from: "https://rr.sapo.pt/noticia/46824/cibercrime-temaumentado-mas-nao-ha-estatisticas", Last Access: 20 December 2018.
18. Cabreiro, C.; Identity theft is growing, Retrieved from: "https://rr.sapo.pt/noticia/46824/cibercrime-temaumentado-mas-nao-ha-estatisticas", Last Access: 20 December 2018.
19. "Online Safety", International Criminal Police Organization (INTERPOL) Retrieved from: "https://www.interpol.int/en/Crime-areas/Cybercrime/Online-safety/Ransomware ", Last Access: 20 December 2018.
20. "Bitdefender next-generation machine-learning and memory introspection technologies ensure that Enterprises worldwide have always been safe from the WannaCry ransomware mega-attack and the underlying Eternal Blue zero-day exploit", Bitdefender, Retrieved from: https://www.bitdefender.com/business/usecases/wannacry.html, Last Access: 20 December 2018.
21. Séneca, H.; "WannaCry: 12 mil computadores infetados em Portugal", Exame Infomática (2017).
22. Justin.; "How to Prevent and Fix WannaCry Ransomware", My Private Network (2018).
23. "No More Ransom", Retrieved from: "https://www.nomoreransom.org/en/index.html", Last Access: 20 December 2018.
24. "What constitutes a cyber-attack?", NEC, Retrieved from: "https://www.nec.com/en/global/solutions/safety/info_management/cyberattack.html", Last Access: 21 December 2018.
25. "; -- have I been pwned?", Retrieved from: "https://haveibeenpwned.com/", Last Access: 22 December 2018.