International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 07 | July 2019 www.irjet.net p-ISSN: 2395-0072

A STUDY ON CYBER CRIMES, CYBER CRIMINALS AND MAJOR SECURITY BREACHES

Mahima Rai[1], H.L.Mandoria[2]

[1,2]*Department of Information Technology, College of Technology, Govind Ballabh Pant University of Agriculture and Technology, Pantnagar, U.S. Nagar*

Abstract - *It can be rightfully said that today's generation lives on the internet. We are living in a digital era where we are constantly using the internet and constantly generating data. This data is stored on the cloud which is basically a huge data server or data center that we can access online. Now for hackers, it is a golden age. This paper explores an overview of cybercrime, how to prevent them also we want to discuss in detail most devastating cyber attacks, top cyber criminals of all the time, countries with most cybercrime and cyber breaches of the 21st century*.

Key Words: **Motivations behind Attacks, types of cyber attacks and their preventive methods, most devastating cyber attacks, cybercriminals, cyber platform, major cyber breaches of the 21st century.**

1. INTRODUCTION

Cyber security is the top concern for today's business owner and technology executives. It can be rightfully said that today's generation lives on the internet. We are living in a digital era where we are constantly using the internet and constantly generating data. This data is stored on the cloud which is basically a huge data server or data center that we can access online. Now for hackers, it is a golden age. Cyber threats are not only increased by the years, but they also are becoming harder to recognize and also evolving with time so they can easily bypass normal antivirus. The Internet is not a safe place as we might think it is. There had been multiple cyber breaches in the past that has compromised privacy and confidentiality of data. Even big companies like eBay, AOL have gone through major cyber breaches even though they have a lot of security measures taken to protect the data. So it's not only that small individuals are targeted by the hackers, but even bigger organizations are constantly being targeted. Former Cisco CEO John Chambers said, "there are two types of companies one who have been hacked and others who don't yet know they have been hacked".

Technological advances are the main driver of economic growth, but they have also resulted in a higher incidence of cyber attacks. Users expect to be always available and always secure in their online experience and their business and personal assets to be safe. Leading trends such as cloud computing, e-commerce, Big Data, and analytics, mobile payments, it, AI, machine learning and social media, all increase the cyber risk to users. A total of 864 breaches was reported, with a total of almost 34.2 million records exposed in 2018 as of September. According to the 2018 Identity Theft Resource Center, the number of records exposed per Data breach averaged 39,554 year - to- date in 2018, with the highest number of records exposed in the business category. According to the IBM Security and Ponemon Institute 2018 Data Breach Study, the average cost of a stolen or lost record continues to rise and is $ 148 worldwide in 2018compared to an average of $ 141 in 2017. IoT devises extensive use increased the cost by $ 5 per compromised record. The U.S. and Canada have the highest data breach cost per capita at $ 233 and $ 202. India and Brazil, at $ 68 and $ 67 respectively, have the lowest cost per capita [1].

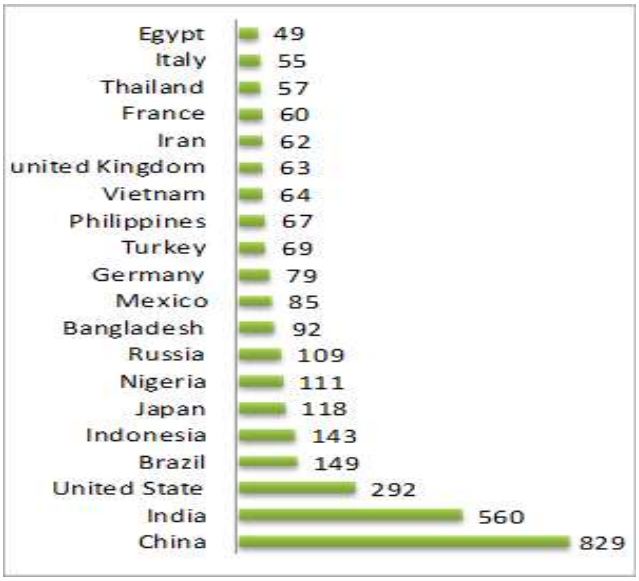

Fig -1: Top 20 countries with the highest number of internet users (in millions)[2]

2. MOTIVATIONS BEHIND ATTACKS

2.1 Cyber crimes

Cybercrime is defined as a crime in which a computer is the object of the crime (phishing, hacking, spamming) or is used as a tool to commit a crime (hate crimes, child pornography). Cybercriminals may use computer technology to access business trade secrets, personal information or use the internet for malicious or exploitative purposes. Criminals can also use computers for document or data storage and communication. Criminals who perform illegal activities on the internet are often referred to as

hackers. It is also being referred to as computer crime.

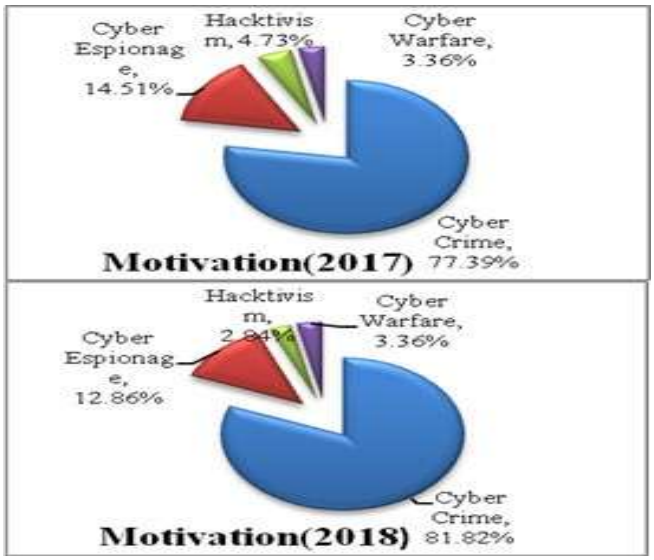

Fig -2: Motivations behind Attack

2.2 Cyber Espionage

Cyber espionage is the practice of spying or using secret agents to obtain information about activities and plan of a foreign government or competing company. Secret agents are armies of hackers from around the world who use cyber warfare for political economic or military gain. These highly valued and deliberately recruited cybercriminals have the knowledge of how to shut down anything from government infrastructure to utilize resources and financial systems. They have influenced the outcome of political elections and helped companies fail and succeed.

2.3 Cyberwarfare

Cyber warfare is any virtual dispute initiated as a politically motivated attack on an enemy's computer and information systems. Executed via the Internet, these attacks disable organizational and financial systems by altering or stealing classified data to undermine websites, networks, and services. Cyber warfare is also known as cyberwar. In these types of attacks, nation-state actors attempt to disrupt the activities of nation-states or organizations, especially for strategic or military purposes.

2.4 Hacktivism

Hacktivism is the act of hacking a computer network or website in an effort to convey a political or social message. Hacktivist is a person who carried out the act of Hacktivism. In contrast to a malicious hacker who hacks a computer with the aim to cause harm or steal private information, hacktivists engage in similar forms of disruptive activities to highlight social or political causes. For the hacktivist, hacktivism is an Internet-enabled policy to exercise civil disobedience. Acts of hacktivism may include denial-of-service attacks (DoS), web- site defacement, redirects, information theft, website parodies etc.

3. TYPES OF CYBER ATTACKS AND HOW TO PREVENT THEM

3.1 Malware

Malware is an all-encompassing term for a variety of cyber attacks, including computer virus, worms, spyware, Trojan horse, adware. Malware is simply defined as a code with malicious intent that typically steals data and destroys something in the computer [3]. The way malware goes about doing its damage can be helpful in categorizing what kind of malware you are dealing with.

Types of Malware:

a) Virus: A computer virus is a program that can copy itself and infect a computer without the permission and knowledge of the user. A computer virus has two major characteristics- the ability to replicate itself and the ability to attach itself to another computer file. A few signs that your computer may have viruses include slow response time, random hard drive crashes, and extensive pop-up ads.

b) Worms: Like a virus, worm also replicates however, it does not infect other files rather it copies itself to other network computers. The worm will do this repeatedly and can cause slowness or even block network transmission. Worm attack weakened points in a network and is difficult to quarantine. The worm's main purpose is to spread. They don't usually target the user's data.

c) Trojan horse: Trojan horse is a type of malware designed to provide unauthorized remote access to a user's computer. The Trojan does not replicate by infecting other files on computers like viruses. Instead, they often survive going unnoticed. They may sit quietly in your computer collecting information. A Trojan horse can steal various data such as credit card information and can also install malware into your system. One of the most common things Trojan can do is creating a back door which makes changes to your security systems so that your data and devices can be accessed by their controller.

d) Spyware: Spyware is a type of malware that is designed to be undetected by the person who is infected. Spyware is difficult to detect. It lies hidden until activated by the person who installed it from the outside. Then it starts recording information about your activities on the computer and then transmits them at a specific time to the users who installed it.

How to stop malware?

a) Updating firewall has constantly been a great idea. The firewall prevents the transfer of large data files over the network in a hope to weed out attachments that may contain malware.

b) It's also important to make sure your computer operating system (e.g. Windows, Mac OS X, Linux) use the most up to date security update. Software programmers update programs frequently to address any holes or weak points. It's important to install all these updates as well as to decrease our own system weaknesses.

c) Stop clicking suspicious links. Always study the URL consciously and make sure you are not on a counterfeit site.

3.2. Phishing

Often posing as a request for data from a trusted third party phishing attack are sent via email and ask the user to click on a link and enter their personal data. Phishing emails have gotten much more sophisticated in recent years and making it difficult for some people to discern a legitimate request for information from a false one. "In past few years, most of the attacks on financial institutions have not been through brute force attacks on firewall appliances, it has been through acquiring user's passwords, this technique is called Phishing". Phishing emails often fall into the same category as spam, but are more harmful[4].

How exactly does Phishing works?

People associate phishing with email messages spoof or mimic bank credit card companies and other companies like Amazon, eBay, Facebook. These messages look authentic and attempt to get victims to reveal their personal information. But email messages are only one small piece of a phishing scam. From beginning to end the process involves the following steps:

The phisher must decide which businesses to target and determine how to get email addresses. Once they know which business to spoof and who their victims are, phishers create methods for delivering the messages and collecting the data. Then they have to execute the attack. This is the step most people are familiar with that is the phispher send phony messages that appear to be from a reputed source. After that, the phisher rackets the information the victims enter into the web page or pop-up window. In the last step which is basically identity theft and fraud, the phishers use the information they have gathered to make illegal purchases or commit fraud [5].

How exactly can we be actually preventing ourselves from getting phished?

The only thing that we can do is be aware of how phishing email actually works. A phishing email has some very specific properties:

a) Firstly, we will have something like a much-generalized way of addressing someone like a dear client.

b) Then our message will not be from a very reputable source. For example, it can be written as amazon.com on the label, but when we actually inspect the email address, it's something like amazonmanagement@mazon.com, which is not a legitimate Amazon address.

c) Thirdly, you can click on redirect links and can see where they actually redirect you too.

3.3 Password Attacks

An attempt to obtain or decrypt a user's password for illegal use is exactly what a password attack is. Hackers can use the cracking program, dictionary attacks and password sniffers in password attacks. Password cracking refers to various measures used to discover the computer password. This is usually accomplished by recovering passwords from data stored in or transported from a computer system. Password cracking is done by either repeatedly guessing the password usually through computer algorithms in which the computer tries numerous combinations until the password is successfully discovered. Password attacks can be done for several reasons, but the most malicious reason is in order to gain unauthorized access to a computer without a computer owner's awareness. This result in cybercrime such as stealing the password for the purpose of accessing bank information.

There are three common methods used to break into a password protected system:

a) Brute Force attack: A hacker uses a computer program or script to try to login with possible password combinations usually started with the ease to guess the password. So just think if a hacker has a company list he or she can easily guess username if even one of the users has a password like 123 he will quickly be able to get in.

b) Dictionary Attacks: A hacker uses a program and script to try to log in by cycling through the combinations of common words. In contrast with brute force attacks where a large proportion key space is searched systematically a dictionary attack tries only those possibilities which are most likely to succeed. Typically derived from a list of words, for example, a dictionary. Generally, dictionary attacks succeed because most people have a tendency to choose passwords which are short or easy.

c) Key logger attacks: A hacker uses a program to track all of the user's keystrokes. So at the end of the day, everything the user has typed including id and password has been recorded. Keylogging program uses malware.

Ways to stop password attacks:

a) Update Passwords: It's always a great idea to keep changing the essential password at regular intervals.

The password should not be the same for everything.

b) No Dictionary: It's always a great idea to use a password that only makes sense to you. Passwords which use actual words that make sense are much more susceptible to dictionary attacks.

c) Use Alphanumeric: When setting a password best practice should be followed. A password should contain a multitude of characters with generous use of alphanumeric.

3.4. Distributed Denial of Service Attack

DDOS attacks are subclasses of denial of service (DOS) attacks. A DDOS attack involves multiple connected online devices, collectively known as a 'Botnet' which are used to overwhelm a target website with fake traffic. DOS attack focuses on disrupting the service to a network as a name suggests. The attacker sends a high volume of data of traffic through the network until the network becomes overloaded and can no longer function. There are a few different ways attackers can achieve DOS attack, but the most common is DDOS. This involves the attacker using multiple computers to send the traffic or data that will overload the system. In many instances, a person may not even realize his/her computer has been hijacked. Disruptive services can have various consequences relating to security and online access. Many instances of large scale DOS attacks have been implemented as a single sign of protest towards governance or individual and led to severe punishment including major jail time [6].

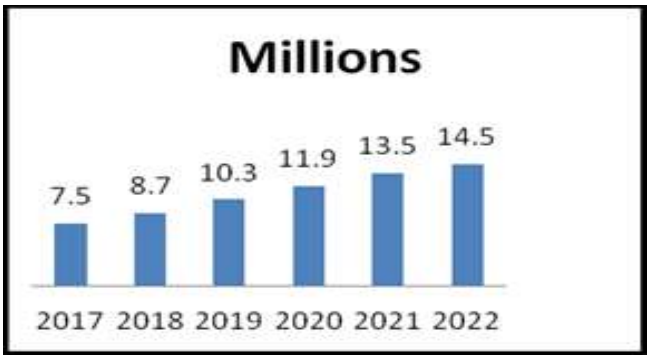

Fig -3: Global DDoS attacks Forecast, 2017-2022

How can we prevent DOS attacks?

Unless your company is huge, it's rare that you would be even targeted by an outside group or attackers for a DoS attack. The best way to prevent an additional breach is to keep your system as secure as possible with regular software updates, online security monitoring and monitoring of your data flow to identify any unusual or threatening spikes in traffic before they become a problem. DOS attacks can also be prevented by simply disconnect the plug that connects your website server to the internet [7].

3.5 Man-in-the-Middle Attack

The man in the middle attack can obtain information from the end users and the entity he or she is communicating with. For example, if you are banking online the man in the middle will communicate with you by impersonating your bank and communicate with the bank by impersonating you. The man in the middle will then receive all of the information transferred between both parties which could include sensitive data such as bank account and personal information[8].

How to prevent Man-in-the-Middle Attack?

Use encrypted WAP i.e. an encrypted wireless access point. Always check the security of your connection (HSTS/HTTPS) because when somebody is actually trying to compromise your security he will try to strip down HTTPS or HSTS that is being injected in the website which is basically security product calls. So if someone like HTTPS is not appearing on your website you are on an insecure website where your information can be compromised. By investing in a virtual private network, which spoofs your entire, IP and you can just browse the internet with perfect comfort.

3.6 Drive-By-Download

Gone are the days where we have to click to accept a download or install a software update in order to become infected. Now just opening a compromised web page could allow dangerous code to install on your devices. Drive-by- download attacks occur when a vulnerable computer gets infected by just visiting a website. Finding from the latest Microsoft security intelligence report and many of its previous volumes reveals that Drive-by exploits have become the top web security threat to worry about. A drive-by-download refers to the unintentional download of a virus or malicious software on your computer or mobile device. A drive-by-download usually takes advantage or exploits a browser or app or operating system that is out of date and has security flaws. This initial code which is downloaded is often very small and since its job is often simply to contact another computer where it can pull down the rest of the code onto the Smartphone, tablets and other computers. Often a web page will contain several different types of malicious code and hopes that one of them will match weakness in your system.

How to prevent drive-By-Download Attack?

The best advice about avoiding Drive-by-Download is to avoid visiting websites that could be considered dangerous or malicious. Some other ways to stay protected include: keep your internet browser and operating system up to date, use a safe search protocol that warns you when to navigate malicious sites and use comprehensive security software [9].

3.7 Malvertising

Malvertising is the name, we in the security industry, give to criminally controlled adverts which intentionally infect people and businesses. There can be an ad on any site often once, which you use as part of your everyday internet usage. It is a growing problem as evidenced by a recent US Senate report and the establishment of bodies like a Trust in Ads. The advertisement looks the same as any other, but has been placed by criminals without your knowledge. A tiny piece of code hidden deep in the advertisement is making your computer go to the criminal servers. Basically, you are redirected to criminal servers, the malware injection takes place.

How to prevent Malvertising?

a) You need to use an ad blocker. You can have the ad blocker extension installed in your browser whether it is chrome, Safari or Mozilla.

b) Regular updates of browser or software always help.

c) If there is an advertisement about a lottery that is offering you free money is probably going to scam you and infect the malware too. So use your common sense and never click on those ads.

3.8 Rogue software

Rogue software is a form of malicious software and internet fraud that misguide user into believing that there is a virus on their computer and manipulates them into paying money for a fake malware removal tool. Also known as Smitfraud, Scareware, or Rogue Security Software this type of software is defined as malware. It is designed specifically to disrupt or damage a computer system. In this case not only is the software going to disrupt your system, but it's also going to trick you into making a purchase using a credit card. Rogue security software has been serious security threats since 2008.

How does it work?

The scams manipulating a user into download program through a variety of techniques. Some of these methods include ads offering a free or trial version of security programs. Once the scareware is installed it can steal all your information, slow your computer or corrupt your files.

How to prevent Rogue software?

Update firewall, use efficient antivirus that can detect threats. And also the general level of distrust on the internet and not actually believing anything

4. MOST DEVASTATING CYBERATTACKS OF THE WORLD

4.1 WannaCry

The WannaCry cyber attack is perhaps the most devastating hack seen so far. WannaCry is a ransomware worm that spread rapidly through across a number of computer networks in May 2017 and shutdown computer system completely. The hackers than an offer to unblock the system for the price and this blackmail was on a global scale. WannaCry affected 300,000 systems in over 150 countries. Hackers demanded 600 dollars with cryptocurrency for each computer which was blocked. The WannaCry ransomware arrives on the infected computer in the form of a dropper, a self-contained program that extracts the other application components inserted within it. Once launched, WannaCry tries to access a hard-coded URL if it can't, it proceeds to search for and encrypt files in a bunch of important formats, ranging from Microsoft Office files to MKVs and MP3s, leaving them unavailable to the user. It then displays a ransom notice, demanding 300 dollars in Bitcoin to decrypt the files. WannaCry spread very quickly using a tool that security experts believe was created by the NSA.

To be clear the NSA was not interested in ransom just in snooping. But they created a tool that took advantage of a security weakness in the Microsoft software. The tool dubbed Eternal Blue exploits vulnerability in the Server Message Block or SMB protocol. The SMB protocol is basically a system for sharing files access across a network and the reason why you might never hear of it is that normally it's totally safe. The NSA discovered that in some versions of windows the SBM protocol can be tricked into accepting packets of data from remote attackers. Eternal Blue was designed to use that flaw as a way in.

4.2 Ashley Madison Hack

In the past years, millions of adults had their personal information exposed as a result of the hack, the Ashley Madison Hack is perhaps most embarrassing cyber attack of all. In 2015 the company Ashley Madison discovered that its private server has been accessed by a hacking group known as "The Impact Team". This group then threatens to release all of the information that they had to the public if Ashley Madison did not shut down the company. The reason for this was Ashley Madison was specialized in allowing married people to have affair discretely. 25GB of user's data was released and this exposed its users publicly. It was also revealed that only 12 thousand of 5.5 million registered users were female and most of those were created from fake IP addresses. 37 million customers had their personally-identifiable information stolen and put on the Internet for anyone to see.

4.3 Mafia Boy Attack

Michael Calce, a 15-year-old boy, in 2000 caused substantial damage to a series of high profile website including Amazon, eBay, Yahoo, Fifa.com, Dell. At the time, Yahoo! was the biggest search engine in the world. He did this through a series of distributed denial of service attack. This type of attack is common. Mafia Boy uses this approach and rendered its target useless for hours. This resulted in millions of dollars with lost revenue. After being sentenced to one year prohibition Michael Calce published a book about his experiences. He says his goal had nothing to do with money. "The overall purpose was to intimidate other hacker groups," says Calce. For the national security apparatus, the attack was a wake-up call. Today Calce is a white hat hacker. Companies hire him to help design better security features and identify security flaws in their systems. He says the internet is a far scarier place today than it was back in 2000. For one, there is more and more at stake as we rely ever more on online systems for our daily lives.

4.4 Soviet Pipeline Explosion

The 1982 Soviet pipeline incidence involves the computer attack which was directly responsible for a massive explosion. During the cold war, Soviet attempted to steal computer software used to oversee pumps in gas pipes, knowing this the CIA placed a Trojan virus inside their software. When Soviet attempted to use the software to operate a massive gas pipeline in Siberia the Trojan horse took control of the walls and closed them. This created a massive amount of pressure, the result being the largest non-nuclear explosion ever seen from the space. There were no casualties but the CIA achieved their dream of disrupting the Soviet gas industry, which had a massive economic impact for them.

4.5 Yahoo Theft

Some cyber attacks are so effective that the victims don't even know that it's happening, that was the case of Yahoo. The one time most popular search engine in the world has seen a number of instances where user data have been stolen by the hackers. This was the biggest hack in the history of the world in terms of scale. Yahoo had an information breach that affected almost a billion accounts. Yahoo reported two major data breaches during the second half of 2016. The data breach reported in September 2016 had occurred in 2014 and an estimated 500 million accounts were hacked. Hacker accessed user name, password as well as other sensitive materials. But unbelievably it took Yahoo four years to discover that even bigger hack has taken place during 2013 which was reported in December 2016 and believed to have affected over 1 billion user accounts and today also nobody knows who is responsible for this.

4.6 Shamoon Virus

Security experts warn that energy suppliers could be targeted by hackers. Such an attack could render a country immobile. Imagine the world with no electricity, this is purely a hypothetical situation. Hackers have already targeted energy supplies in the past. The Shamoon virus was developed in 2012 and was released by a group of hackers who called themselves the "Cutting Sword of Justice". The virus was used to undermine the energy company "Saudi Aramco". When the virus was released it infected more than 30 thousand computers in the company shutting down the entire network. The virus erased data on three-quarters of Aramco's corporate PCs, spreadsheets, e-mails, files and replacing all of it with an image of a burning American flag. To make things worse the virus spread to other energy companies.

4.7 The Sony Hack

Also known as "the Sony Picture Hack". This 2014 cyber attack from North Korea made international headlines. The hacker group called themselves "Guardian of Peace (GOP)" and leaked confidential information from the film studio Sony Pictures. The data included information about copies of unreleased Sony films, personal information about Sony pictures employees, information about employee salary and other confidential information. In November 2014, the Guardian of Peace group demanded that Sony drop out its film "The Interview", a comedy about a plot to kill North Korean leader "Kim Jong-un". Destover malware was used to harm Sony Pictures which acts as a backdoor and was capable of wiping disk drives and any Master Boot Record disk. Sony canceled the film's formal premiere and mainstream release.

4.8 Titan Rain

It was during early 2000, the cyber attacks began to ramp up with Titan Rain. Being the most notorious, this virus targeted American computer networks and affected a number of US government contractors such as Redstone Arsenal, Lockheed Martin, Sandia National Laboratories and it even spread to NASA. The virus transmitted sensitive information to an unknown source. This included highly classified technology, which is still under development. The UK also found itself under an attack from Titan Rain and firmly pointed the finger at China as a source.

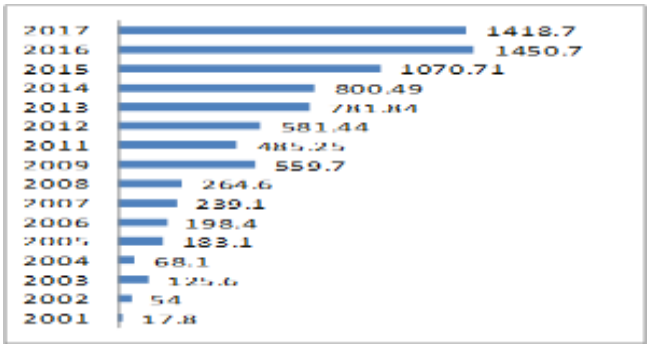

Fig-4: Amount of monetary damage caused by reported cybercrime from 2001 to 2017 (in million U.S. dollars) reported to the IC3

5. CYBER CRIMINALS

Cybercriminals are individuals or group of people who use technology like digital system or network to commit malicious activities with the intention of stealing confidential information for the number of reasons like generating profit, taking revenge, etc. There is a number of cybercriminals based on their hacking skills and they are listed in Table I.

Table -1: Types of Cyber Criminals

Types of Cybercriminal	Description
White Hat Hackers	Use their hacker skills for defensive purposes, also known as security analysts and have permission from systems owner.
Black Hat Hackers	Individuals with extraordinary computing skills, resorting to destructive or malicious activities, also known as Crackers
Gray Hat Hackers	Falls somewhere between black hats and white hats have both good and bad intentions and work both offensively and defensively.
Green Hat Hackers	These hackers are non-professional in the hacking world. They have desired to learn and become a perfect hacker.
Blue Hat Hackers	They have no desire to learn and their main motive is to take revenge.
Red Hat Hackers	Like white hats, they use their skills for defensive purposes, but are ruthless towards black hats.
Script Kiddies	A hacker who compromises systems using widely distributed computer programs or scripts, rather than using their own programs and scripts
Suicide Hackers	Individuals who aim to bring down the critical infrastructure for a cause and are not worried about facing jail terms or any other kind of punishment.
Cyber Terrorists	Individuals with a wide range of skills, motivated by political or religious beliefs to create fear by large scale disruption of computer networks.
State Sponsored Hackers	Individuals employed by the government to penetrate and gain top secret information and to damage information systems of other governments
Hacktivist	An Individual who promotes a political agenda by hacking, especially by defacing website
Malicious Insider Or Whistleblower	Individuals hired by rivals to collect trade secrets of their opponents.
Corporate Spies	They use their hacker skills for commercial or financial purposes instead of purely national security

6. CYBER PLATFORM

Platforms connect people, there are different sites and companies that facilitate connections between consumers and suppliers. Cybercriminals are using these platforms as a source for data theft and hacks. Yahoo's breeches were the largest in recorded history and compromised up to 3 billion user profiles. Recently, Facebook has been in the news for a high profile data leak. Cybercriminals know where to look for data.

Table-2: Some Major Data Breaches of 21st Century through Social Sites/Industries [10]

Sites/ industries	Types of sites/industries	Number of users compromised	Year
Yahoo	American web service provider	3-billion	2013-2014
Marriott International	Hospitality Company	500 million	2014-2018
Adult friend finder	Online dating, Adult Entertainment	412.1 million	2016
Under Armour	Apparel, accessories	150 million	2018
ebay	Multinational e-commerce corporation	145 million	2014
Equifax	Credit risk assessment	143 million	2017
Target Tore	Retailer	110 million	2013
Facebook	Online social media and social networking service company	87 million	2018
Anthem	Health insurer	78.8 million	2015
Sony Play Station	Japanese multinational conglomerate corporation	77 million	2011
JP Morgan Chase	American multinational investment bank and financial services company	76 million	2014
Uber	Transportation network Company	57.6 million	2016
Home Depot	American home improvement supplies retailing company	56 million	2014
Adobe	American multinational computer software company	38 million	2013

7. CONCLUSION

Not all people are a victim but all are still in risk to cyber crimes. With the advancement in technology, criminals don't have to go outside to commit a crime or they don't need any physical weapon. They have everything on their computers. There are many ways criminals can commit cyber crimes. In this paper, we have seen how cybercriminals have committed crimes using their computer skills. There must be some sort of mechanism and protocol to protect us from all these sorts of cyber attacks and there is a way called Cyber Security.

REFERENCES

[1] https://www.statista.com/statistics/267132/total-damage caused-by-by-cyber-crime-in-the-us/

[2] http://www.enigmasoftware.com/top-20-countries-the-most-cybercrim

[3] Ramdinmawii, E., Ghisingh, S. and Sharma, U.M., 2014. A Study on the Cyber-Crime and Cyber Criminals: A Global Problem. International Journal of Web Technology,, 3, pp.172- 179.

[4] Brody, R.G., Mulig, E. and Kimball, V., 2007. PHISHING, PHARMING AND IDENTITY THEFT. Academy of Accounting & Financial Studies Journal, 11(3).

[5] Maghu, S., Sehra, S., and Bhardawaj, A., Inside of Cyber Crimes and Information Security: Threats and Solutions

[6] Nicholson, L.J., Shebar, T.F. and Weinberg, M.R., 2000. Computer crimes. Am. Crim. L. Rev., 37, p.207.

[7] Douligeris, C. and Mitrokotsa, A., 2004. DDoS attacks and defense mechanisms: classification and state-of-the-art. Computer Networks, 44(5), pp.643-666.

[8] Desmedt, Y., 2011. Man-in-the-middle attack. Encyclop edia of cryptography and security, pp.759-759.

[9] Nykodym, N., Taylor, R., and Vilela, J., 2005. Criminal profiling and insider cyber crime. Computer Law & Security Review, 21(5), pp.408-414.

[10] https://www.csoonline.com/article/2130877/the-biggest data-breaches-of-the-21st-century.html