iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VI **Month of publication:** June 2020

DOI: http://doi.org/10.22214/ijraset.2020.6305

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VI June 2020- Available at www.ijraset.com

Understanding Cybercrime and its Consequence Worldwide

Tanishq Verma[1], Dhruv Garg[2]
[1, 2]*Amity University, Uttar Pradesh, Noida, India*

***Abstract:** In today's world, (www) or the World Wide Web, the Internet is used by almost everyone around the world for getting small information to large money transactions. The internet was invented to benefit the world but it can now being misused. This paper presents a comprehensive and systematic review of Cyber Crime and it's consequence worldwide. This paper reviews that can be incorporated in the system according to specific needs.*
***Keywords:** Cybercrime, Most familiar types of cybercrime, Statistics of cybercrime worldwide, Prevention of cybercrime.*

I. INTRODUCTION

Cybercrime also known as computer-oriented crime is an unlawful act that involves computer and network. It is also known as the offences that are committed against single or a group of people with a criminal mind set to deliberately hurt the stand of an organisation or a company or cause damage to individual through internet or world wide web. Cybercrime also affect the nation's security. Cybercrime are generally used for personal growth while some are carried out in case of vengeance and other may also be carried out as impact on finance. Cybercriminals also known as hackers may select a particular single or an organisation's data and then sell it for its own benefits. Cybercrime involves crimes like Financial Fraud, cyber extortion, cyber terrorism, cyber warfare, online harassment and drug trafficking are the most frequent types of cybercrime committed globally. The exponential increase in number of electronic devices world are leading to gradual increase in the crime committed over the internet too. Internet and computer together can wreck the civilization or an organization that are in the distance of our creative power.

II. MOST FAMILIAR TYPES OF CYBERCRIME

Cybercrime can have different identities and it is almost impossible to fight it. Every year hackers and cybercriminals are making different techniques to or evolving new ways to penetrate the life of an individual or an organization for their own interest keeping not only there personal information but also account number, password and other at risk.
It's anything but difficult to move toward becoming overpowered in the event that you have been a casualty if a cybercrime, however the initial step is to comprehend what kind of cybercrime you have been focused with and the sort of data conceivably undercover.

The most common types of cybercrime are

A. Computer fraud
B. DDos attack
C. Ransomware

III. COMPUTER FRAUD CYBERCRIME

Computer Fraud is the most frequent type of cybercrime which involves a computer to change the data or to gain access to restricted data in the computer. Computer Fraud involves sending hoax email or electronic mail, accessing to the classified information from unauthorized computer, accessing in data mining through software like spyware or through malware, attacking and exploiting the weakness of the security system of the computer to unlawfully access personal details of the individual such as credit card details, bank account details, social security number and other personal data. It also involves dispatching viruses or worms that when run reproduces itself with aim to destroy another party computer or network.
Computer Fraud also includes online e-commerce, online share trading, mobile banking, digital banking, crypto currency and internet banking financial frauds cybercrimes. Computer fraud are effortless and frequent and it is almost impossible to detect and the hacker cannot be tacked back if not informed immediately.

©IJRASET: All Rights are Reserved

IV. DDOS ATTACK

DDos Attack or Distributed Denial of Service Attack is a computer crime in which the attacker or the hacker's main aim is to load the malware into computer such as IoT devices making each of the devices a bot. DDos attack can also be done by loading a trojan instead a malware and are aimed at a single system causing denial of service. The attacker then has control over the bot network also known as the botnet. DDos attack is a cyber attack and one of the most frequent form of cyber crime in which the hacker makes the network resources unavailable temporarily interrupt the service of the host. Cybercriminals or Hackers aims for the sites of high profile organization such as banks, MNCs. The main motive of the hacker is revenge to an organization or blackmail to the organization demanding ransom.

There are many categories of distributed Dos attack such as Traffic attacks, Bandwidth attacks and Application attacks. In Traffic attack the hacker infects the computer with high number of TCP packets. In Bandwidth attack the hacker sends the targeted computer with massive amount of junk data. In Application attack the hacker deplete the information in the application layer.

V. RANSOMWARE

Ransomware is a kind of malicious software either a malware created to restrict access to computer data and the computer network until some ransom is given to the hackers or cybercriminals. It is a normally dispatched through phishing electronic-mail or by accessing an infected website. Ransomware can be dangerous to any individual or an organization. The individuals or any organizations which includes multinational companies and even some of the state government department's data/personal information stored can be at a risk of being attacked by the cybercriminals.

Ransomware can also be defined as a small part of a malware where the personal information of the victim is interlocked by the hackers through encryption and a ransom is demanded to get back the data. The main motive of the attacker is monetary and the demand of the ransom is given through digital currency such as bitcoin so that the attacker identity is safe and cannot be tacked. The attacker after getting the ransom gives instructions to the victim to get back control of it's information.

There are different types of ransomware which include

1) *Scareware:* It is a type of ransomware in which the victim device get a pop-up saying that the device is infected with a typical malware. Ignoring to such a pop-up leads to many more pop-ups.
2) *Screenlocker:* It is the most common type of ransomware in which the victim gets locked out of his own computer and does not have any access. It looks like an official government software that can only be fixed by paying fine and so the victim does pay fine. The official government does not have any indulgence in this, they might not even know about it till the victim get them informed.
3) *Doxware:* In this type of ransomware the attacker intimidate the victim to get his personal information public if he does not pay the ransom.

VI. EFFECTS OF CYBERCRIME WORLDWIDE

According to the recent study and report form all around the world, the updated statistic shows that the amount that is impacted by cybercrime is more than the income of most of the countries. It is estimated that approximately about $4.2 trillion in 2016, about14% tax on growth. As the crime grown exponentially, cybercrime has been ranked as the third most infected crime in the world behind government corruption and narcotics. The most common reasons are-

1) *It is Everywhere:* About 2/3 of the people who are using the internet get affected by cybercrime, i.e there personal data is stolen or at risk.
2) *Low Risk-High Profit:* The probability that a person has attempted a cybercrime and goes to jail very low. Most of the hackers who have attempted cybercrime have knowledge about it and keep there identity protected from the world and so it is difficult to track them down.

Ransomware is a rapid growing cybercrime that has more than 6000 online criminal marketplaces that are selling product and service that conduct such type of cybercrime. According to Federal Bureau of Investigation approximately $209 million in ransom is estimated with almost more than $24 million in 2015. The reason for such a rapid growth are-

a) Ransomware kits and tools are easy to used and can be founded easily as well. There are almost 600 illegal online criminal marketplace where you could find tools and devices to conduct a cybercrime.
b) RaaS – RaaS known as Ransomware as a Service where you can find small organization which can conduct a ransomware for you and instead can get a cut out of the total ransom. This make more opportunites for a person to take revenge with another person without disclosing his/her identity.

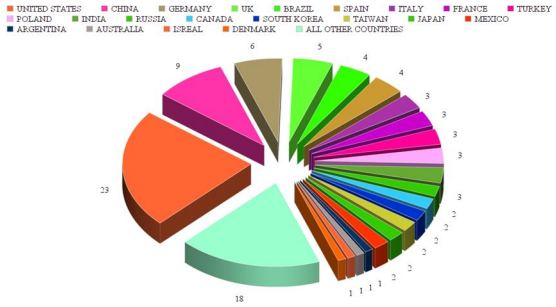
©IJRASET: All Rights are Reserved

c) WannaCry- WannaCry a ransomware software that when spread through a website or a network can lead to looking multiple device connected to that network.

According to the worldwide report the estimated number of cybercrime in North America, Europe, Central Asia, East Asia, and the Pacific, South Asia, Latin America and the Caribbean. It is described and predicted through the report that the number of cybercrime that are occurring in these continents are depends on the cyber security measure taken by the respective government which includes legal measure, technical measure, organization measure and capacity building. Cybercrime results are divided into three tiers. These are top tier, mid tier and the beginning stage.

The top tier are the countries with have good cyber security and have digital economies. The mid tier consist of the countries which are evolving and making their cyber security strong. The beginning stage are the countries which have cyber security at the beginning level. There are some countries which are impacted largely by cyber attacks. These are-

- Brazil- According to study, brazil is second leading source of cyber attacks.
- Japan- Japan is a country which was not impacted by cyber crime because of the communication/ language barrier. But today as we see, there is a rapid increase in attacks targeting banks.
- United Kingdom- Approximately 5.5 million dollars has been impacted in UK through online frauds considering almost half of all the crimes committed in the country.
- United Arab Emirates- Cyber crime cost country about 1.4 billion dollar per year and is the second most effected country worldwide.



Cybercrime has a great impact on economical growth, jobs, innovation and investment. It is estimated that approximately 95% of the cybercrime victim has not reported the crime due to any personal reasons and this make the hackers and cybercriminal even more prompt to attempt more cybercrime. Cybercrime is allowing low level hackers and attackers to easily make money from an individual and organization. Some of the biggest cyber attacks has be discussed.

A. Cyber Attack at Sony

The one of the biggest successful enterprises Sony in April of 2011, was attacked. Sony's PlayStation

Network which is a multiplayer gaming service provided by Sony was attacked which has information of all the users subscribed to PSN. The network system had personal information of about 77 million users which was at stake. The attackers demanded about 15 million dollars as a ransom. Sony had to pay the ransom plus the money that the attacker used the card of the customer who were using PSN as a compensation as well as some of the legal charges. But again in November 2014, a part of the Sony, Sony's Picture Entertainment was attacked by a malware or a computer worm by a hacker organization which happens to call themselves as "GARDIANS OF PEACE". They stole about 100 TB of data from Sony which consist of personal information of about 49,000 employees working at Sony to confidential information including film scripts.

B. Marriott Hotels attacked

Marriott Hotels the world's leading hotel company was cyber attacked compromising the personal information of up to 500 million guests worldwide including their banking data. Marriott got to known that they were attacked when a breach was alerted in September 2018 in their database when someone was trying to access the confidential information of the Marriott. The information of the Marriott customers in the database was at stake and ransom was demanded. The personal information contained details such as backing details, email, phone number , address , passport number and also SPG account which is a high end credit card launched by American express to frequent travellers. Marriott now face a fine of about 123 million dollars by UK government over this breach.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VI June 2020- Available at www.ijraset.com

VII. FUTURE PREDICTIONS OF CYBERCRIME

Cybercrime is a crime which has high profit and low risk meaning that any attacker or hacker can earn a lot or make money easily without getting his identity disclosed or getting caught. According to the study, there is an increase in the cyber attacks on individual to organization yearly. The future prediction also states that there will be even more crime occurring the coming year. However the government and the organization will be at it's best to reduce such cyber attacks. 2018 shows that there has been a rapid increase in the attacks on individual and organization. Facebook has also reported that nearly 30 million people information has been stole from it database. Cyber crime is inevitable and it can only be reduced to a certain extent or degree. Research show that there are some activities that can happen which will most likely to disturb or damage the organization.

A. Hackers will make the most of AI to assault

Artificial intelligent will be used by many organization to make use of the automated work and help automate manual task and enhance decision making and help human with other activities. However, AI can also be used by hackers for their own personal benefits as many AI are used to keep the server and database of the organization. Hackers will not only find a solution and destroy AI to get control of the information of personal individual and organization but will also use AI tools to boost their cyber attacks. Attackers can use AI to detect vulnerabilities in the system, can be used in phishing and other attacks and can also use AI to make exactly realistic audio and video and even well drafted emails that could fool the individual in believing this as true. Toolkits are easily available online and can make it easy for criminals to create new crimes.

B. New 5G technology will give hacker new area to attack

As we known that the coming year is all about 5G technology and how will it give high speed internet performance to the user. But it is important to understand that how this technology works. After complete establishment of 5G all over world, more 5G IoT devices will be connected directly to the 5G network instead of connecting it to WiFi router which will make it more vulnerable to attack

C. Hackers will exploit supply chain

This work when hacker infects a fake legitimate software upgrade packet with malware. Such hacker are present at the production of the software chain. When this infected software package is distributed to all the victims around the world, it will automatically get the computer infected giving control of the computer to the hacker. These type of attacks are increasing at unexpected rate and it is very difficult to predict such type of attack.

D. Capture data in transit

It likely to be seen that hacker will exploit the home WiFi router and other unsecured IoT devices. After the devices are infected it will capture data passing through it. Malware is inserted into there types of router could help steal banking credential, capture credit card no, and other useful information for the hacker. We can expect the hackers to continue and find numerous ways from capture data in transit.

E. Preventions of cyber attack

Cyber attack is a crime that cannot be completely varnish but can only be reduced or prevented. Organization are investing more and more in cyber security so that cyber attack can be prevented. Here are some common steps that can reduce cyber attack at an individual-

1) *Do Not Share Your Personal Information*- Keep your secret safe and do not share your information with others. Sharing your personal information such as banking information or house address, family information on an unsecured site can lead to a cyber attack at you. The best way to check if the sites is secure or not is to look for s in the websites url. Example of a secured site will have a url as "https:".
2) *Do Not Just Open Up Emails And Download Files From It*- Opening unknown emails and downloading of files can lead to installing of viruses into your computer. If you are secure or know the person in general then you can download or reply to the email. Some emails even lead to an unsecured sites which will look similar to a usual site and so will ask for your banking detail. In this case it is best to call up the company and ask about the email.

©IJRASET: All Rights are Reserved

3) *Not Keeping System Up To Date*- It is another important reason which gives attacker to attack your computer. Not updating to latest software update can lead to hackers finding a bug in previous software and so can will give them opportunity to attack. So it is important to keep your system to automatic update.
4) *Keeping Backup*-It is important to keep your system backed up while installing any other type of software into your computer. New hacking techniques are getting discovered steadily and so it can effect your computer. If you keep you data backed up to a secured cloud storage or any other storage devices like hard disk then it will keep your data safe if in any case your data does get encrypted.
5) *Perform Penetrating Test*- Organization and large MNCs are putting a lot of money to keep the data secured and keeping them safe from cyber attack. Checking and performing vulnerabilities and penetrating test will help you to check how secured your software or website is. Usually the organization perform this whenever they are about to launch a new software but some of the cloud service organization perform this on regular bases like monthly.
6) *Proper Insurance*- Despite from just protecting your software or website it is important for you to keep your organization safe by keeping it insured whenever a cyber attack occurs. The insurance company will be liable to pay the damages in case of any break in the security. Some of the cyber attacks make large companies a loss of lot of money and can so reduce it by insuring itself.

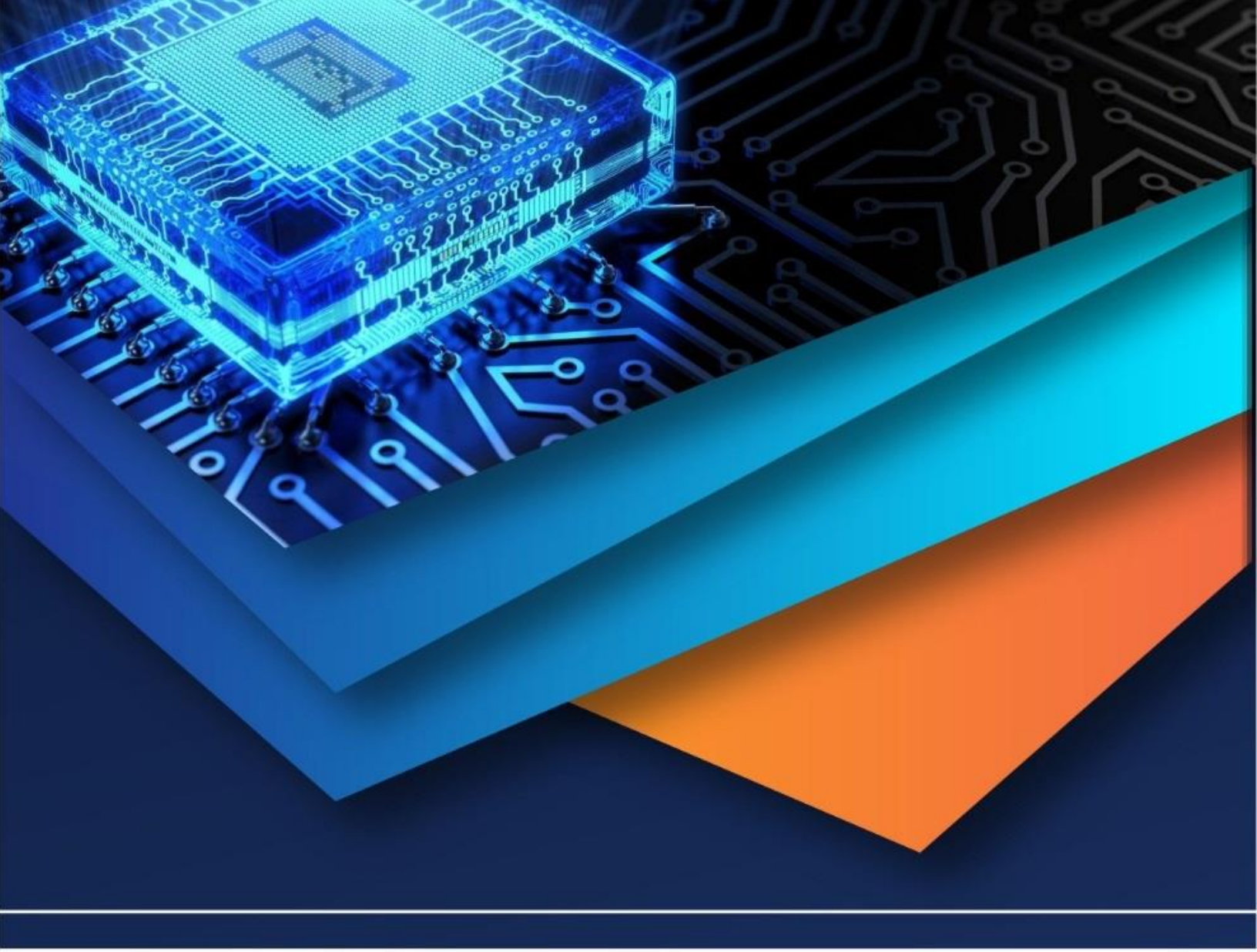
VIII. CONCLUSION

Internet giving us so much opportunities, it is also important to understand that it also gives hackers a chance to make cyber attacks. We have already studied that cyber attacked cannot be destroyed completely but can only be reduced to a certain degree. As the technology is evolving so will the techniques of cyber crime too. This paper presents a comprehensive and systematic review of understanding cyber crime and its impact worldwide. This paper reviews that can be incorporated in the system according to specific needs.

REFERENCES

[1] McAfee “together is power”, executive summary - The Economic Impact of Cybercrime “ No Slowing Down”.
[2] Building Better Commerce Website introducing topic “ Financial Impacts of Cybercrime” copyright Merchant Risk Council.
[3] ZD Net article of website ”Cybercrime drains $600 billion a year from global economy, says report” 2019 CBS interactive All Rights Reserved Indian Edition.
[4] Outpost 24 Internet Article “ TOP 10 of the world largest cyber attacks” published on 03 December 2019 AAA Highest Creditworthiness.
[5] Wikipedia (The free encyclopedia) article webpage of “ Gurdians of the Peace” refrences from Pro Governmwnt Militias Database.
[6] Symantec Blogs / Feature Stories posted on 28 November 2018 article “ Cyber Security Prediction : 2019 and Beyond” by 2019 Symantec Corporation.
[7] IT ProPortal website article of “ 10 Essential steps to prevent cyber attacks on your company “ published on June 13, 2018 by Alex Tyler.
[8] Varonis.com , “ 60 must-know cybersecurity statistics for 2019” by Rob Sobers Updated posted date 17/04/2019
[9] E-Pulse Blog, “ Preventing cyber attacks through Efiicient cyber resilience” written by Harry Bodd published by Externet Works .
[10] Nojitter, “ cyber security posted by country : US. Not the best” by Gary Audin published on 15 February 2019 by infoma tech 2019 UBM Americas.
[11] us-cert.gov “ Ransomware” article by CISA, a part of the Department of the Homeland Security, An official website of the Department of the Homeland Security.
[12] The Free Dictionary By FARLEX “ computer crime “ CITE Collins Dictionary of LAW W.J. Stewart , 2006
[13] cloudflare,.com “ what is DDos attack ?” by 2019 Cloudflare, Inc.
[14] viciimconnect.org, “Financial fraud crimes” office of the justice, U.S department of justice “NATIONAL CENTER FOR VICTIM OF CRIME”
[15] Journal.elsevier.com by Elsevier “most downloaded computer fraud and security articles” copyright 2019 elsevier B.V .
[16] Voipshield “utmost defence against cyber attacks “ a journal by Erika Hernandez published on 14th February 2018 , “ the 16 most common types of cybercrime acts”,
[17] Finextra.com by finextra , financial fraud crimes and cyber crime : can banks stay one step ahead?” published on 23 august 2018 by Monica Hovsepian.
[18] Searchsecurity.techtarget.com ,” bybercrime, posted by Margaret Rouse by TechTarget 20.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)