Cyber Crime

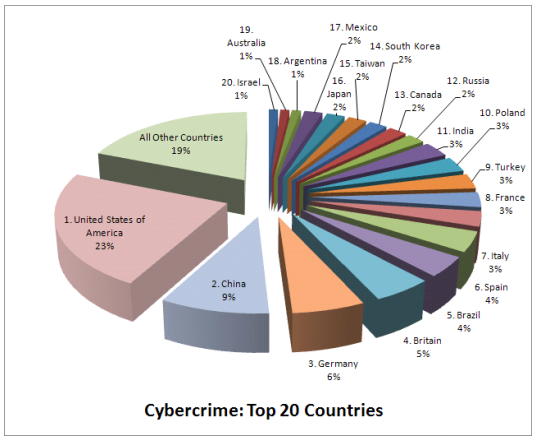
Anant Jain, Namit Gupta
CCSIT, TMU, MORADABAD
jain1999anant@gamil.com
namit.k.gupta@gmail.com

***Abstract*--As we all know that cyber crime has been one of the most common activity made by the computers experts. In this paper I have mentioned some of the impact of cyber crime .Cyber crime are that activities made by the people for destroying organizations for network stealing and other valuable data , documents ,hacking banking details. My paper includes detailed information regarding cyber crime and modes of cyber crime. Finally i will go for the research on the crimes made by the misuse of internet in some of the areas like Financial crimes ,Cyber pornography, E-mail spoofing, E-mail bombing, virus attacks .Finally I will get the main objectives of my paper. Like this my paper will be complete.**

Introduction

Cybercrime, also called computer crime, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government. Computer crime has been an issue in criminal justice and criminology since the 1970s, criminals use computers to commit crimes. Cybercrime is a criminal act using a computer that occurs over the Internet. The Internet has become the source for multiple types of crime and different ways to perform these crimes. The types of cybercrime may be loosely grouped into three categories of cybercrimes. First, the Internet allows for the creation and maintenance of cybercrime markets. Second, the Internet provides a venue for fraudulent behavior (i.e., cyberfraud). Third, the Internet has become a place for the development of cybercriminal communities.

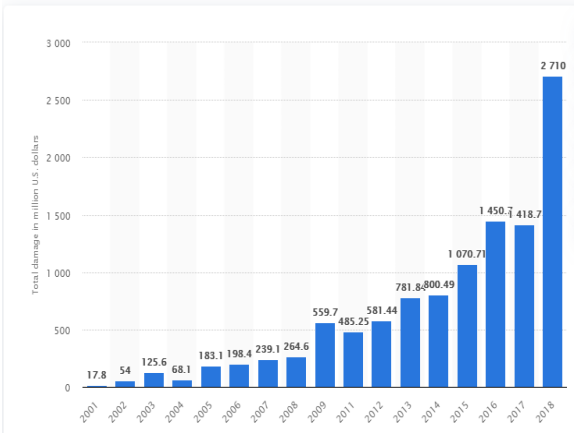
Facts about the Cybercrime market:
The World Economic Forum (WEF) has listed cyber attacks as the third most likely global risk in 2018 and given the lucrative market for cyber criminals this is not going to scale down in the coming years. According to Forbes, the global information security spending is poised to hit $124 billion by 2019, mainly driven by privacy concerns and regulations. The scenario of a considerable rise in the cybercrime activities has put huge pressure on industry players. If the cyberattacks have increased, then it must be noted that the attack vectors have also proliferated – from emails, websites to IoT devices and weaponization of AI-enabled devices, its all-pervasive leaving them vulnerable. New age threats like ransomware, cryptojacking for cryptomining, attacks on cyber-physical systems involving critical infrastructure such as power grids, transportation systems and other areas are lethal. Similarly, the old methods like phishing attacks and malware infection are equally damaging for any business.



Top 20 Countries Found to Have the Most Cybercrime

The costs of cybercrimes are mind boggling – loss, theft, manipulation of data, data processing infrastructure, theft of money, identity, intellectual property, personally identifiable data, digital forensic investigations, loss of productivity, reputation loss for organizations, fines, penalties, damages and law suits for organizations, loss of customers leading to dip in revenues, cost of restoration activities to bring business operations to normalcy are some of the ways in which these cybercrimes prove that they are dangerous. There have been times when business could not identify a malicious code written in a complex manner and hence, they incurred heavy losses or had to temporarily suspend business services. Some of the other impacts are that the key executives were removed from their positions and even had to face prison time which further damaged their reputation in the eyes of the public.

Damages done by Crime Globally:



Amount of monetary damage caused by reported cyber crime to the IC3 from 2001 to 2018
(in million U.S. dollars)

It is already been touted that the cybercriminal activity is going to be the biggest challenge that mankind will face in the next few decades. It is estimated that cybercrimes will cost $6 trillion annually (up from $2 trillion in 2015) in 2021. It is interesting to note that as per the Cost of Data Breach Report, 2018 of Ponemon Institute, the average total cost rose from $3.62 to $3.86 million, an increase of 6.4 percent from 2017 and the average cost for each lost record rose from $141 to $148 in 2018. The prediction is that these numbers would only grow in the years to come.

Most common types of cybercrime:

1. Malware

Over half (55%) of all types of cybercrime involve malware, according to the report. These attacks include spyware and remote administration malware. From there, they can gain login credentials, sensitive business data, or information to help them conduct social engineering attacks. The third most popular kind of malware attack is the dreaded ransom ware, which typically locks your device or takes your data hostage until you pay the hacker to release it.

2. Social engineering

Social engineering attacks (31%) don't rely on technical sophistication so much as trust. Because they prey on human vulnerabilities instead of technological ones, this type of cybercrime is especially difficult to guard against. Types of social engineering attacks include phishing and more elaborate physical schemes.

3. Hacking

Typically the term hacking encompasses a wide variety of attacks. Positive Technologies defines it more narrowly in its report: "attacks that take advantage of vulnerabilities in software and services, weaknesses in protection mechanisms, and other shortcomings of targeted systems that do not involve social engineering or malware."

4. Web attacks

Web attacks represent fifth of cybercrimes against businesses. These attacks exploit vulnerabilities in websites to access the data of other users of the sites. For example, hackers might inject malicious code into an e-commerce website that allows them to steal customers' credit card information.

5. Credential compromise

Seventeen percent of attacks involved credential compromise, meaning a hacker uses your login information to gain unauthorized access to your accounts. An attacker can learn your credentials in a number of ways: phishing, social engineering, malware (such as key loggers), or hacking (gaining access to a database of credentials and cracking the passwords).

6. Distributed denial of service (DDoS)

Although few businesses will ever find themselves the target of a DDoS attack (2%), these can be extremely costly and disruptive. DDoS attacks flood a network with traffic, overwhelming it and preventing legitimate users or employees from accessing the service. Once the network is effectively shut down, the hackers typically demand a ransom to restore service.

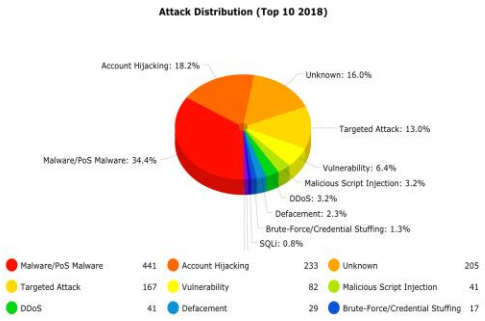
7. Malicious Code – Viruses, Worms and Trojans

Virus: - A virus is a program that modifies other computer programs. These modifications ensure that the infected program replicates the virus. Not all viruses cause damage to its host. A virus is typically spread form one computer to another by e-mail, or infected disk. However a virus cannot infect another computer until the program is executed. A common method of virus execution is when a computer user is tricked into opening a file attacked to an e-mail, thinking the file is a harmless program coming from a friendly source. The most popular example of virus is the Melissa virus which was launched in March 1999. The Melissa virus was hidden in a Microsoft word attachment that appeared to come from

a person knows to the recipient. The program activated a macro that tread the first fifty e-mail addresses located in the Microsoft Outlook e-mail program and e-mailed itself to the fifty addresses. The virus was estimated to have caused $80 million in damages.

Worms:-A worm is standalone program that replicates itself. A worm can wind its way throughout a network system without the need to be attached to a file, unlike viruses. For example: I love you worm in 2001 was estimated the loss caused to be $US 10.7 billion.

Trojans: - A Trojan Horses is an innocent looking computer program that contains hidden functions. They loaded onto the computer's hard drive an executed along with the regular program. However, hidden in the innocent program is a sub-program that will perform an unauthorized function. A Trojan horse is the most common way in which viruses are introduced into computer systems. For example: Back Orifice 2000 is a program designed for misuse and attack on another computer.



"***The modern thief can steel more with a computer then with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than a bomb.***"

How to protect yourself from web attacks globally?

Some of the security measures are given below:-

Use an Internet Security Suite: If you know anything at all about a computer and the internet, the chances are very high that you might be using an antivirus already (And if not then do not take the risk unless you are seasoned cyber security professional with data backups in place). An antivirus program combined with an internet security program set helps you in:

1. Use an Internet Security Suite:

If you know anything at all about a computer and the internet, the chances are very high that you might be using an antivirus already (And if not then do not take the risk unless you are seasoned cyber security professional with data backups in place). An antivirus program combined with an internet security program set helps you in:

- Avoiding malicious downloads done by mistake.
- Avoiding malicious installs done by mistake.
- Preventing from being a victim to Man in the Middle Attack (MITM)
- Protection from phishing.

2. Use Strong Passwords:

This can't be emphasized enough. If you have "qwerty123" as your bank's password and a lot of money in the account, you must be ready for a surprise transaction. You should not fully rely on the rate-limiting measures used by websites that you visit. Your password should be strong enough to be practically unbreakable. A strong password is one that is 12+ characters long and contains a diverse use of alphabets(both cases), numbers and symbols (and spaces). Setting a really unbreakable password should not be difficult specially when there are help available as random password generators.

3. Keep Your Software Up-to-Date:

Despite the developer's best intention to create secure software and thorough reviews from the security teams, there are unfortunately many zero-days that are revealed once the software is being used by a large user base. Companies are well aware of this fact and that is why they release frequent updates to patch these vulnerabilities. This is the reason why those updates, however annoying they may be, are important. They help in preventing attacks that can easily skip the radar of the antivirus programs on your computer.

4. Avoid Identity Theft:

Identity theft is when someone else uses your personal information to impersonate you on any platform to gain benefits in your name while the bills are addressed for you. It's just an example, identity theft can cause you to damage more serious than financial losses. The most common reason for identity theft is improper management of sensitive personal data. There are some things to be avoided when dealing with personally identifiable data: Never share your Aadhar/PAN number (In India) with anyone whom you do not know/trust .Never share your SSN (In US) with anyone whom you do not know/trust. Do not post sensitive data on social networking sites. Do not make all the personal information on your social media accounts public.Never share an Aadhar OTP received on your phone with someone over a call. Make sure that you do not receive unnecessary OTP SMS about Aadhar (if you do, your Aadhar number is already in the wrong hands) Do not fill personal data on the website that claim to offer benefits in return.

How India uses many prevention methods against Cyber Crime:-

Generally India made many Cyber Laws against these Cyber Crime happened in present scenario. These laws are made to protect all the citizens of India against very serious crimes.All these laws are made to protect people from all Traditional criminal activities are such as theft, fraud, forgery, defamation, and mischief are part of cyberspace. Cyber Laws in India prevent any crime done using technology, where a computer is a tool for cybercrime. The laws for cybercrime protects citizens from dispensing sensitive information to a stranger online.

Some of the Laws are as follows:-

1. Copyright Law:

In relation to computer software, source code, websites, cell phones contents etc.

2. Licensing Law:

In terms of software and source code.

3. Trademark Law:

With relation to domain names, meta tags , mirroring, framing , linking etc.

4. Semiconductor Law:

Which relates to the protection of semiconductor integrated circuit design and layouts.

5. Patent Law:

In relation to computer hardware and software.

6. Data Protection and privacy Law:

Aim to achieve a fair balance between the privacy rights of the individual and to interests of data controllers such as banks, hospitals, email service providers.

Ever since the introduction to cyber laws in India happened, IT Act 2000 was enacted and amended in 2008 covering different types of crimes under cyber law in India.

The main purpose of this act is to provide legal recognition of electronic commerce and to facilitate filing of electronic records with the government.

ITA 2008, as the new version of Information Technology Act 2000 is often referred, has provided additional focus on Information Security. It has added several new sections on offences included Cyber Terrorism and Data Protection .

Conclusion

Criminal behaviour on the Internet, or cybercrime, presents as one of the Major challenges of the future to India and International law enforcement. It already feature in many international crime involving drug trafficking, people smuggling, terrorism and money laundering. Digital evidence will become more commonplace, even in traditional crimes, and we must be prepared to deal with this new challenge. Law enforcement agencies around the world are working together to develop new partnerships, new forensic methodologies and new responses to cybercrime in order to ensure safety and security on the Internet. New skills, technologies and investigative techniques, applied in a global context, will be required to detect, prevent and respond to cybercrime. This "new business" will be characterized by new forms of crime, a far broader scope and scale of offending and victimisation, the need to respond in much more timely way, and challenging technical and legal complexities. Innovative responses such as the creation of „cyber cops“, „cyber courts“ and „cyber judges“ may eventually require to overcome the significant jurisdictional issues. To prevent from all of these web attacks, there are some laws mainly based on people's concern around the world which helps them to secure their information and data from many unauthentic users around the world. Cyber law in India is not a separate legal framework. It’s a combination of Contract, Intellectual property, Data protection, and privacy laws. With the Computer and internet taking over every aspect of our life, there was a need for strong cyber law. Cyber laws supervise the digital circulation of information, software, information security, e-commerce, and monetary transactions.

Refrences

[1] Artical on Cyber Crime written by : Michael Aaron Dennis, ENCYCLOPAEDIA BRITANNICA.

[2] https:www.myadvo.in/blog/what-is-the-cyber-law-in-india-byMYADVO.

[3] Cyber Crime control by-https:security boulevard.com.

[4] How to Protect Yourself From Cyber Attacks? – Geeks for Geeks

[5] How to Prevent Cyber Crime in India? - MyAdvo.in

[6] Cyber Crime introduction by - Information Security and Cyber Law, by Poonam Singh.