International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 12, Issue 3 [March. 2023] PP: 116-118

Cyber Crime: A crime against computers and Devices

Vishnupriya Dadhich
(Assistant Professor)
B. N. University, Udaipur

Abstract-
Cybercrime is a criminal activity which involves a computer, networked device or a device. Some cybercrimes carried out against computers or devices directly to damage or disable them and other cybercrimes use computers or devices to spread malware, illegal information, images or other materials. Some cybercrimes do both like- target computers to infect them with a computer virus which is spread to other machines and sometimes entire network.
Keywords- *Cybercrime, Criminal activity, Computer network, Device, Malware, Illegal, Virus.*

Date of Submission: 03-03-2023 Date of acceptance: 15-03-2023

Meaning of cybercrime- It is a computer and network device criminal activity. The necessity of internet connectivity has enabled an increase in the volume and pace of cybercrime activities because the criminal no longer needs to be physically present when committing a crime. The internet's speed, convenience, anonymity and lack of borders make computer based variations of financial crimes- such as ransom ware, fraud and money laundering, as well as crimes such as stalking and bullying- easier to carry out. Cyber criminal activity may be carried out by individuals or groups with relatively little technical skill, or by highly organized global criminal groups that may include skilled developers and others with relevant expertise. To further reduce the chances of detection and prosecution, cybercriminals often choose to operate in countries with weak or nonexistent cybercrime laws.

The Council of Europe Convention on Cybercrime (CECC) defines cybercrime as a wide range of malicious activities. It includes the illegal interception of data, system interference that compromise network integrity and availability and copyright infringements.

The U.S. Department of Justice (DOJ) has divided cybercrime into 3 categories, which are-

(a) To target the computer device for crimes, example- to gain network access

(b) In some crimes the computer is used is the target, example- to launch a denial-of-service (DoS) attack

(c) Where the computer is used as an accessory to a crime, example- using a computer to store illegally obtained data.

Types of Cybercrime- There are many different types of crimes. Most cyber crimes are carried out with the exception of financial gain by the attacker though the ways cyber criminals aim to get paid can vary.

1) **DDoS Attacks**-These are used to make an online service unavailable and take the network down by overwhelming the site with traffic from a variety of sources. Large networks of infected devices known as Botnets are created by depositing malware on user computers. The hacker then hacks into the system once the network is down.

2) **Botnets**- Botnets are networks from compromised computers that are controlled externally by remote hackers. The remote hackers then send spam or attack other computers through these botnets. Botnets can also be used to act as malware and perform malicious tasks.

3) **Identity Theft**- This cybercrime occurs when a criminal gains access to a user's personal information to steal funds, access confidential information or participate in tax or health insurance fraud. They can also open a phone/internet account by anyone's name, use name to plan a criminal activity and claim government benefits with name. They may do this by finding out user's passwords through hacking, retrieving personal information from social media, or sending phishing emails.

4) **Cyber stalking**- This kind of cybercrime involves online harassment where the user is subjected to a plethora of online messages and emails. Typically cyber stalkers use social media, websites and search engines to intimidate a user and instill fear. The cyber stalker knows their victim and makes the person feel afraid or concerned for their safety.

5) Social Engineering- Social engineering involves criminals making direct contact with person usually by phone or email. They want to gain confidence and usually pose as a customer service agent so person will

give the necessary information needed. This is typically a password, the company that person work for, or bank information. Cyber criminals will find out what they can about person on the internet and then attempt to add that person as a friend on social accounts. Once they gain access to an account, they can sell person's information or secure accounts in your name.

6) PUPs- PUPS or Potentially Unwanted Programs are less threatening than other cyber crimes but are a type of malware. They uninstall necessary software in your system including search engines and pre downloaded apps. They can include spyware or adware, so it is a good idea to install an antivirus software to avoid the malicious download.

7) Phishing- This type of attack involves hackers sending malicious email attachments or URLs to users, to gain access to their accounts or computer. Cyber criminals are becoming more established and many of these emails are not flagged as spam. Users are tricked into emails claiming they need to change their password or update their billing information, giving criminals access.

8) Prohibited/Illegal Content- This cyber crime involves criminals sharing and distributing inappropriate content that can be considered highly distressing and offensive. Offensive content can include, but is not limited to, sexual activity between adults, videos with intense violent and videos of criminal activity. Illegal content includes materials advocating terrorism related acts and child exploitation material. This type of content exists both on the everyday internet and on the dark web, an anonymous network.

9) Online Scams- These are usually in the form of ads or spam emails that include promises of rewards or offers of unrealistic amounts of money. Online scams include enticing offers that are "too good to be true" and when clicked on can cause malware to interfere and compromise information.

10) Exploit Kits- Exploit kits need a vulnerability (bug in the code of a software) in order to gain control of a user's computer. They are readymade tools criminals can buy online and use against anyone with a computer. They are readymade tools criminals can buy online and use against anyone with a computer. The exploit kits are upgraded regularly similar to normal software and are available on dark web hacking forums.

11) Cyber extortion- A crime involving an attack or threat of an attack coupled with a demand for money to stop the attack. One form of cyber extortion is the ransom ware attack. The attackers gains access to an organizations systems and encrypts its documents and files, anything of potential value, making the data inaccessible until a ransom is paid. This is in some form of crypto currency, such as bitcoin.

12) Crypto jacking- An attack that uses scripts to mine crypto currencies within browsers without the users consent. Crypto jacking attacks the may involve loading crypto currency mining software to the victim's system. However, many attacks depend on Java Script Code that does in-browser mining if the user's browser has a tab or window open on the malicious site. No malware needs to be installed as loading the affected page executes the in-browser mining code.

13) Identity theft- An attack that occurs when an individual access a computer to glean a users personal information, which they then use to steal that person's identity or access their valuable accounts. Such as banking and credit cards. Cyber criminals buy and sell identity information on darken market, offering financial accounts, as well as other types of accounts, like video streaming services, webmail, video and streaming, online auctions and more. Personal health information is another frequent target for identity.

14) Credit Card Fraud- An attack that occurs when hackers infiltrate retailers systems to get the credit card and/or banking information of their customers. Stolen payment cards can be bought and sold in bulk on darknet markets. Where hacking groups that have stolen mass quantities of credit cards profit by selling to lower level cyber criminals who profit through credit card fraud against individual account.

15) Cyber espionage- A crime involving a cyber criminal who hacks into systems or networks to gain access to confidential information held by a government or other organization. Attacks may be motivated by profit or by ideology, cyber espionage activities can include every type of cyber attack to gather, modify or destroy data as well as using network connected devices, like webcams or closed-circuit tv (CCTV) cameras to spy on a targeted individual or groups and monitoring communications including emails, text massages and instant messages.

16) Software piracy- An attack that involves the unlawful copying, distribution and use of software programs with the intention of commercial or personal use. Trademark violations, copyright infringement and patent violations, copyright infringement and patent violations are often associated with this type of cybercrime.

17) Exit Scam- The dark web has given rise to the digital version of an old crime known as the exit scam. Dark web administrators divert virtual currency held in marketplace escrow accounts to their own accounts essentially, criminal stealing from other criminals.

18) Unauthorized Access and Hacking- Unauthorized access means any kind of access without the permission of either system or computer network. Hacking means an illegal intrusion into a computer system and/or network. Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use readymade computer desire to destruct and they get the kick out of such destruction.

19) Web Hijacking- Web hijacking means taking forceful control of another person's website. In this case the owner of the website loses control over his website and its content.

20) Pornography – Pornography means showing sexual acts in order to cause sexual excitement. The definition of pornography also includes pornographic websites, pornographic magazines produced using computer and the internet pornography delivered over mobile phones.

21) Child Pornography- The interest is being highly used as a medium to sexually abuse children. The children are viable victim to the cyber crime. Computers and internet having become a necessity of every household, the children have got an easy access to the internet. There is an easy access to the pornographic contents on the internet.

22) Cyber Stalking- Stalking can be termed as the repeated acts of harassment targeting the victim such as following- the victim making harassing phone calls, killing the victims pet, vandalizing victim property, leaving written messages or object. Stalking may be followed by serious violent acts such as physical harm to the victim. Cyber stalking means repeated acts of harassment or threatening behavior of the cyber criminal towards the victim by using internet services.

Reference-

[1]. https://www.techtarget.com/searchsecurity/definition/cybercrime
[2]. https://www.techtarget.com/searchsecurity/definition/cybercrime
[3]. https://www.jigsawacademy.com/blogs/cyber-security/types-of-cyber-crime/
[4]. Information Technology Act, 2000