Research on Recent Sensitive Cybercrimes

Pavithra N[1], Dr C Thiyagarajan[2]
[1]Dept of Computer Science
[2]Associate Professor, Dept of Computer Science
[1, 2] PSG College of Arts & Science, Coimbatore, India

Abstract- *Modern day economic, commercial, cultural, social, and political activity is mostly conducted online on all scales. For many commercial enterprises and governmental organizations around the world, the subject of cyber attacks has recently become problematic. Cybersecurity is necessary to reduce the risk of cyberattacks and prevent the unlawful use of systems, networks, and technology. This study aims to understand various forms of cybercrimes, cyberattacks, and security methods to counter them.*

Keywords- Cyber attack, Cyber security, Data breach, Data Privacy, Cyberspaces.

I. INTRODUCTION

The term "Cybercrime", is defined as the use of a computer, for illegal acts that include, fraudulent data access, the trafficking of child pornography, theft of intellectual property, identity theft, and privacy violations. Internet-based social networking services are becoming a target for hackers [3]. Crimes are classified against the humans, property and nation. These classified crimes include stalking, pedophilia, copyright issues, computer terrorism.

Knowledge on Cyber crimes helps to protect oneself from assault, to protect your data, from jeopardizing cyber attacks. Thousands of devices all over the world can be easily affected with single threat. Therefore, individuals and organizations should implement the essential safeguards to prevent their sensitive information from ending up in the hands of rivals or criminals. To assure safety and security on the Internet, law enforcement agencies from all around the world are collaborating to create new partnerships, new forensic procedures, and new responses to cybercrime.

Today, a lot of countries and governments are setting strong rules in place to stop the loss. Cybersecurity education is considered as essential requirement. Governments and market economies, as well as international trade, travel, and communications, have all been impacted by technology. The below Figure , shows that the crime rate of cyber attacks are gradually increasing from 2012 to 2021 in India.

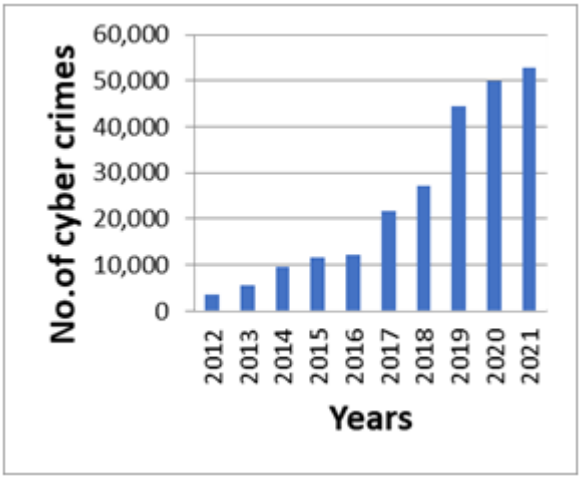

Fig 1 Crime rate of cyber attacks

II. TYPES OF INTRUSION

Today's globe is subject to a wide variety of cyber threats. It is simpler for us to defend our networks and systems against different sorts of cyber attacks if We are aware of them. The below represented table 1 shows the type of cyber attacks and their prophylaxis.

Table 1: Types of Cyber Attacks

TYPES OF ATTACK	DESCRIPTION	EXAMPLE	PREVENTION
Malware attack	Malware attacks are frequent cyberattack s in which malicious software (often malware) causes the victim's machine to carry out illegal acts.	Worms, Spyware, Ransomware, Adware, Trojans.	Implement antivirus software. Install firewalls. Keep an eye out for questionable links, and stay vigilant.

Phishing attack	Phishing is a sort of cyber security assault where bad actors send messages posing as a reliable individual or organization.	The fake invoice scam. Email account upgrade scam. Advance-fee scam.	Examine the emails you get carefully. Utilize an anti-phishing toolbar. Regularly change your password

- Informational obstruction,
- Counter International cyber security measures,
- Slowdown the decision-making process,
- Refusing to provide public services,
- Reduction in public confidence, Nation's reputation will be damaged,
- Splintering the legal Interest.

III. GOALS AND MOTIVES BEHIND CYBER ATTACKS

The data or information on governmental websites, financial institution websites, online discussion forums, news and media websites, and websites for military and defense networks are the primary targets of cyberattacks.

Cyberattacks have specific goals and objectives, they are:

A. *Informational obstruction:*

When specific data or information is required, the attacker's primary goal is to prevent access to essential information of any organization. The ability of the company or government to plan and carry out future events is compromised since the attacker will prevent the authorized user from accessing the information.

B. *Counter International cyber security measure:*

Any significant cyber attack's key goals are to contest and outwit the international cyber security community's initiatives to limit or stop cyberattacks. Attackers try to accomplish this by making their attacks more sophisticated and intricate or by blending their programmes into regular operations to get around security.

C. *Slowdown the decision-making process:*

Cyber attacks are a significant factor in the paralysis of vital sectors such as the military and emergency services, which delays important decisions like tactical deployment and the activation of life support, which may result in fatalities or military defeats.

D. *Refusing to provide public services:*

Attackers can disrupt industries including banking, railway and airline services, stock markets, and government information by preventing authorized users from obtaining data pertaining to public services from any firm or from the government.

E. *Reduction in public confidence:*

There has been a significant decline in public confidence in an organization's security or dependability as a result of hacking or information theft.

F. *Nation's reputation will be damaged:*

One of the main goals of cyberattacks is to harm a nation's reputation. Every Country now has technologically advanced capabilities that raise its status among other developing nations. If a large- scale cyberattack manages to breach a nation's networks, however, this prestige might be severely damaged.

G. *Splintering the legal Interest:*

One of the reasons for cyber attacks is to destroy work that has been formally approved. The security objectives must be correctly specified in order to combat cyberattacks.

IV. RECENT ATTACKS

December 2022, Rackspace Ransomware Attack, Users were having trouble logging into their Exchange Environment, which was later determined to be a ransomware attack, according to Rackspace Technology[4]. Still, there are no signs that any user-sensitive data may have been taken. Security experts claim that the Exchange cluster's unpatched version, which gave attackers access to the ProxyNotShell vulnerability, was to blame for the ransomware outbreak.

2019, PEGASUS, Facebook filed a lawsuit against NSO on the grounds that Pegasus had been used to eavesdrop on the WhatsApp conversations of several activists, journalists, and government officials in India, raising suspicions about

possible collusion between the Indian government and these individuals. 17 people, including journalists, academics, and human rights campaigners, verified to an Indian website that they had been singled out[5].

September 2022, Uber's Internal Systems Compromised By An 18 Year Old, Internal systems at Uber were hacked. The hacker was able to access the company's Slack account, Hacker One account, and complete admin access to its AWS Web Services and GCP accounts. The entrance attack used a social engineering strategy to target Uber's employees. Some of Uber's internal systems were briefly suspended as a result of the breach, and the company is still looking into the situation.

September 2022, Sensitive NATO Data Leaked After Cyber Attack A local Portuguese news outlet, Diario de Noticias, revealed that the Department of Defense of the Portuguese Government had been the target of a major data breach including the release of secret NATO papers that were then made public and sold on the dark web. It was determined following an inquiry that data was transmitted through insecure methods. A bot network that was primarily made to gather sensitive data was used to launch the attack through which the data were exfiltrated. The attack was made to be unnoticed.

October 2022, **Russian Hacktivists, Killnet, Take Down US Airport Websites**, A group of pro-Russian hackers took credit for breaking into many US airport websites. Although this was widely known in our online communities, the infamous "Killnet" hacker outfit just launched another DDoS attack on US airport websites. A pro-Russian hacker group called Killnet is well-known for carrying out DoS (denial of service) and DDoS (distributed denial of service) assaults against public and commercial organizations in a number of nations during the Russian invasion of Ukraine in 2022.

January 2022, Twitter Zero-Day Exposed Data Of 5.4 Million Accounts, Twitter, a social media platform, experienced a zero-day vulnerability that gave hackers access to 5.4 million accounts' personal data. Although the flaw was being used in December 2021, it was discovered by HackerOne's bug bounty program and reported to Twitter in January 2022[7]. Even though the user has blocked this operation in the privacy settings, the vulnerability enables any party to obtain a Twitter ID of any user by providing a phone number or email.

March 2022, Ronin Hack, The creators of the blockchain NFT game Axie Infinity, Sky Mavis, claim that the Ronin Network was the target of one of the biggest DeFi breaches to date. 173,600 ETH and 25.5 million USDC, totaling over $624 million, were taken by the attackers[8]. Private keys were stolen, which allowed for the Ronin Network hack.

2018, Marriott Breach, When Marriott bought the Starwood Hotels organization, a cyberattack had been brewing for some time, but it wasn't revealed until 2018. But by that time, the attacker still had access to visitors' private information. This resulted in an 18.4 million pound fine for the Marriott Hotels from the UK's data privacy authorities. Names, addresses, phone numbers, birth dates, email addresses, and encrypted credit card information of hotel guests were among the leaked data. A smaller set of guests' travel histories and passport numbers were also recorded. It had an impact on around 500 million people. The 2013 Yahoo data breach, which affected three billion user accounts, was claimed to be the second-largest loss of personal data in history after the Marriott data leak.

September 2022, 2.4 TB Data Leak Caused By Microsoft's Misconfiguration, Microsoft has 2.4 TB of data stored in an improperly configured public bucket, according to SOCRadar. 65,000 entities from 111 nations were affected. Data from 2017 through August 2022 is disclosed. According to Microsoft, SOCRadar overstated the extent of the data leak.

V. CONCLUSION

With an increase in internet users, there is also an increase in cybercrime. There are numerous types of cybercrimes that occur on a daily basis. However, most people are unaware of all of these types. Most people are only familiar with hacking and viruses/worms. They are unaware of phishing, cyberstalking, defamation, identity theft, etc. It is essential in today's world to be aware of the crimes associated with the internet.

According to the study, 48% of users share personal information with people they don't know well. 55% of respondents agreed that viruses frequently damage their computers. Spam emails, phishing calls, and emails requesting sensitive information such as mobile numbers, bank accounts, addresses, and so on plagued internet users. It is each of our responsibility to understand the fundamentals of cyber security. Cyber security refers to the technologies and processes designed to protect computers, networks, and data from unauthorized access and cyber-criminal attacks carried out via the internet. People need to understand the fundamentals of cyber security, including:

a. Installing security suites to safeguard the computer from threats like viruses and worms, such as Kaspersky antivirus, McAfee antivirus, Norton Antivirus, etc.
b. Turn on the firewall, antivirus software, and network threat protection.
c. Whenever possible, use alphanumeric passwords that are strong. It's always a good idea to change your password frequently.
d. Never open attachments, download files, or click on links in emails from unknown senders.
e. Beware of pop-ups and links in emails that request personal information.
f. Make sure your computer's operating system and antivirus software are both updated.
l. To prevent becoming a victim of cybercrime, it is the individual's responsibility to stay aware of significant security breaches.
m. Two-step verification for social media and email accounts can stop hackers from breaking into accounts.

REFERENCES

[1] M. Uma-"A Survey on Various Cyber Attacks and Their Classification"-2013
[2] Nina Godbole-"Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives"-2011
[3] Raj Singh Deora - "Brief Study of Cybercrime on an Internet"-2021
[4] URL-https://purplesec.us/security-insights/top- cyber-attacks-2022/
[5] URL-https://en.wikipedia.org/wiki/Pegasus_(spyware) [6]URL-https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks
[6] URL-https://en.wikipedia.org/wiki/2020_Twitter_account_ hijacking
[7] URL-https://halborn.com/explained-the-ronin- hack-march-2022/