Research Inventy: International Journal of Engineering And Science
Issn (e): 2278-4721, Issn (p):2319-6483, PP: 28-37
www.researchinventy.com

Different Threats in Cyber World

Muskan kumari (mkkumari20190000@gmail.com)
Jhumpa chakraborty (affectionatejhumpa@gmail.com)
Muskan ladiya (muskanladiya6202@gmail.com)
Anjali kumari (anjalikumari37612@gmail.com)
Bharti kumara (bharti121323@gmail.com)
Komal kumari (komal9576165742@gmail.com)
Sankit sinha (sankit1532@gmail.com)
Department of CSE, Techno International Batanagar

Abstract:-
Cyber attacks have become common in the era of internet. And it is getting increased every year and damage from this is also increasing. Basically we can say cyber security threats are growing in frequency , diversity and complexity. Providing security against cyber-attacks becomes the most notable things of this digital world. So we can say that , ensuring cyber security is an extremely complex task as it requires more information like domain knowledge about the attacks and capability of analysing the possibility of threats . The main challenge of cybersecurity is the evolving nature of the attacks. Our paper mainly present the different threats in the cyber world that are in the current digital era and cyber security. The analysis made for cyber-attacks and their statistics shows the intensity of the attacks. Various cybersecurity threats are presented along with the machine learning algorithms that can be applied to cyber attacks detection.

***Keywords**:- Worms, Threats , Phishing, Malware , Man in the middle , SQL Injection , Spyware , Ransomware , Denial of service attack ,Zero day Exploit, Advanced persistent Threats, DNS attack, Social engineering attacks , Cyber security issues, Cyber security challenges.*

I. Introduction:-

A cyber security threat is a harmful act which is used to damage data, steal data , or disrupt digital life. Cyber threats consists of computer viruses, data breaches and other attack vectors. Cyber threats is the possibility of cyber attack which is done successfully and which aim to gain unauthorized access, damage, disrupt, or steal an asset of information technology , computer network , intellectual property or any other form of sensitive data. Cyber threats mainly done within an organization by trusted users or in the remote locations by unknown parties Now a days economy and critical infrastructure have become largely dependent on computer network and information technology solution. This is the reason why cyber attacks become more attractive and potentially more disaster because our dependency on information technology increasing day by day. According to the Symantec cybercrime report published in April 2012 cyberattacks cost US$ 114 billion each year .If the time lost by companies trying to recover from cyberattacks is counted, the total cost of Cyberattack would reach around us$385 billion. Victims of cyberattack are also growing. Based on the survey conducted by Symantec which involved interviewing 20,000 people across 24 countries,69% reported being the victim of a cyberattack in their lifetime .Symantec calculated that 14 adults become victim of a cyberattack every second ,or more than one million attacks everyday .

Different Threats in cybersecurity:-

A cybersecurity threat is a harmful attack which is done on purpose by an individual or organization to gain unauthorized network to damage, disrupt, or steal IT assets, computer networks, intellectual property, or any form of sensitive data .

Types of cyber security threats are :-

The types of cyber threats continue to grow, there are some of the most common cyberthreats are [1]1)Malware

Malware attacks are the most common cyber security threats.

Malware is a malicious software, including spyware, ransomware, viruses, and worms, which gets installed into the system when the user clicks a dangerous link or email. Once inside the system, malware can block access to critical components of the net work, damage the system, and gather confidential information, among others.

some of the main types of malware attacks

Viruses- In an application a piece of code injects itself. The code get executed when application runs.

Worms-It is a malware which utilize software vulnerability and backdoors to gain access to an operating system. Once it installed in the network , the worm can carry out attacks .

Trojans-Malicious code or software which poses as an innocent program, hiding in apps , games or email attachments. An unsuspecting user downloads the trojan by allowing it to gain control of their device.

Cryptojacking- attackers deploy software on a victim's device and start using their computing resources to generate cryptocurrency , without the knowledge of victims . And it affect the system due to which the system become slow and it also affect the system stability.

2)Phishing

Cybercriminals send malicious emails that seem to come from legal or valid resources. The user is then tricked into clicking the malicious link in the email, leading to malware installation or disclosure of sensitive information like credit card details and login credential.

3)Spear Phishing

Spear phishing is a more advanced form of a phishing attack in which cyber criminals target only privileged users such as system administrators and C-suite executives.

4)Man in the Middle Attack

Man in the Middle (MitM) attack occurs when cybercriminals place themselves between a two-party communication. Once the attacker interprets the communication ,they filter and steal sensitive data and return different responses to the user.

MitM attacks include:

Session hijacking – An attacks hijacks a session between a network server and a client. The attacking computer substitutes its IP address for the IP address of the client . The server believes it is corresponding with the client and continues the session.

Replay attack – a cybercriminal eavesdrops on network communication and replays messages at a later time, pretending to be the user.

IP spoofing – an attacker convinces a system that it is corresponding with a trusted entity . The system provides the access to the attacker. The attacker forget its packet with the IP source address of a trusted host rather than its own IP address.

Eavesdropping attack- attackers control the insecure network communication to access information transmitted between client and server. It is difficult to detect these attack because network transmissions appear to act normally.

5)Denial of Service Attack

Denial of service attacks is to overwhelm the resources of a target system and cause it to stop functioning , denying access to its users. DDoS is variant of DoS in which attackers compromise a large number of computers or other devices, and use them in a coordinated attack against the target system.

Methods of DDoS Attack include:

Botnets- Hacker control the system that has been infected with malware. Attackers use these bots to carry out DDoS attacks.

Smurf attack – In this attack attacker send internet control message protocol(ICMP) echo requests to the victim's IP address. The ICMP requests are generated from spoofed IP address . Attackers automate this process and perform it at scale to overwhelm a target system.

TCP SYN flood attack – In this attacker attacks flood the target system with connection requests . When the target system attempts to complete the connection , the attackers device does not respond forcing the target system to time out.

6)SQL Injection

A Structured Query Language(SQL) injection attack occurs when cybercriminals attempt to access the database by uploading malicious SQL scripts . Once successful, the malicious actor can view , change , or delete data stored in the SQL database.

7)Zero–day Exploit

A zero-day attack occurs when software or hardware vulnerability is announced, and the cybercriminals exploits the vulnerability before a patch or solution is implemented.

8)Advanced Persistent Threats(APT)

An advanced persistent threats threat occurs when a malicious actor gains unauthorized access to a system or network and remains undetected for an extended time.

9)Ransomware

It is a malware attack in which the attacker locks or encrypts the victim's data and threatens to publish or block access to data unless a amount is paid.

10)DNS attack

It is an attack in which cybercriminals exploits vulnerabilities in the domain name system(DNS).The attackers leverage the DNS vulnerabilities to divert site visitors to malicious pages (DNS Hijacking) and remove data from compromised systems(DNS Tunneling)

11) Social engineering attacks

This attack work by psychologically manipulating users into performing actions according to an attackers .

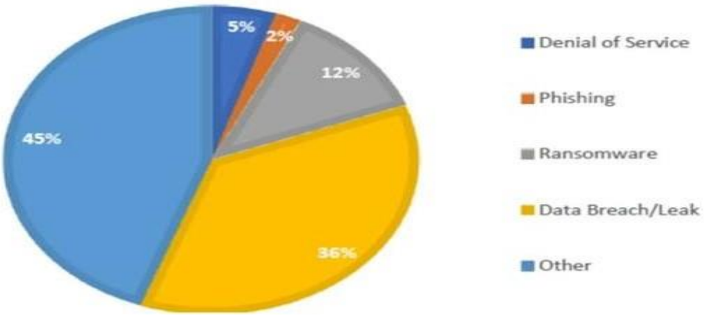
Social engineering attacks include:

Malvertising – Hackers control the online advertising wgich contain malicious code that infects a usrs computer when they click or even just view the add .Malvertising has been found on many leading online publication.

Wiper malware – It intends to destroy data or systems by overwriting an entire file system. Wipers are usually intended to send a political message, or hide hacker activities after data exfiltration.

Rogue security software – pretend to scan for malware and then regularly show the user the fake warnings and detections . Attackers may ask the user to pay to remove the fake threats from their computer to register the software.

Rogue security software – pretend to scan for malware and then regularly show the user the fake warnings and detections . Attackers may ask the user to pay to remove the fake threats from their computer to register the software.



Literature Review :-

The major problem of cybersecurity is not new but rather has developed more than 4 half century the arrest of an east German spy in IMBs German by west Germans police in 1968 was acknowledged as the first case of cyber espionage .[2] In 1983, high school student that was driven by wargame movies and called their selves as successfully got inside the unclassified military networks . Ten years ago, "The first real war in cyber space " attacked Estonia and put the country into " A national security situation" (Hasen and Niessenbaum,2010)[2]. Now a days ,cyber security has been a daily issue that can be found anywhere ,from the news that report spam, scams , frauds , and identity theft to academic articles . Nevertheless , it remains a complicated task to approach a cyber security as merely a simple issue of 'network security' or 'individual security' as it connects to a large issue of 'The state', 'Society' " " 'the nation' and 'the economy.

Cyber security is a compound issue. There is an extensive literature on the series discussing how it can be connected to many different matters that contribute to the development of cyber study and practices.

The profits from the cyber crime are whopping and has become a substantial business over the years . With the advancement in digital ,economic resources and broad amount of open resource tools, attacks have also been trailblazing side by side. The dire need of having the effective mechanism to detect, block and counteract sophisticated threats can not only guarantee to convoy the reputation of the organizations but also shelter the coffers.

Major driving force for these types of cybercrime is money. Majority of the cyberthreats prose to those on the higher level of economic productivity. One of the effective measures to sabotage these attacks would be to block and infiltrate their ability to reach the target and destroy their bottom line productivity.

The attackers often choose the kind of target that ensures a better profit on their investment. The attackers try to stay clear of the complex defences.

The cut to the chase, the organizations should be well aware of the cyber attackers advanced techniques, having a forensic research on the alleged attackers and clear insights into how a certain organizations defence failure.

Cyber threats growing day by day and causing trillions worth of losses to the cyber world. The some important facts, figures, and statistics are:-

- The global average cost of a data breach is **USD 3.92 million[3]**
- Estimated annual losses through cyberattacks to reach **USD 6 Trillion** by 2021[3]

- Cybercrime breaches to increase by **76%** by 2024[3]
- Over **50%** of all global data breaches to occur in the United States by 2023[3]
- The average cost of a data breach to a US company is **USD 7.91 million[3]**
- The average number of days to identify an incident in 2019 was **206 days[3]**
- **2 billion records** were exposed due to data breaches in the first half of 2019[3]
- A business will fall victim to a ransomware attack every **11 seconds** in 2021[3]
- Cyberattacks on IoT devices increased by **300%** in 2019[3]

Cybersecurity Issues:-

The growing role of artificial intelligence (AI) – AI is proving to be both a boon and a bane , it is improving security solutions at the same time it is leveraged by attackers to bypass those solutions. Part of the reason for this is the growing accessibility to AI. In the past, developing machine learning models was only possible if you had access to significant budgets and resources. Now, however, models can be developed on personal laptops.

This accessibility makes AI a tool that has expanded from major digital arms races to everyday attacks. While security teams are using AI to try to detect suspicious behaviour, criminals are using it to make bots that pass for human users and to dynamically change the characteristics and behaviours of malware.

The cybersecurity skills gap continues to grow – Increase in the cybersecurity skill gap has been issue of concern for quite a few years now. There are simply not enough cybersecurity experts to fill all of the positions needed. As more companies are created and others update their existing security strategies, this number increases.

Modern threats, from cloned identities to deep fake campaigns, are getting harder to detect and stop. The security skills required to combat these threats go far beyond just understanding how to implement tools or configure encryptions. These threats require diverse knowledge of a wide variety of technologies, configurations, and environments. To obtain these skills, organizations must recruit high-level experts or dedicate the resources to training their own.

Cybersecurity Challenges:-

Mobile devices are difficult to manage and secure – Even if people haven't fully embraced smart technologies, nearly everyone has a mobile device of some sort. Smartphones, laptops, and tablets are common. These devices are often multipurpose, used for both work and personal activities, and users may connect devices to multiple networks throughout the day.

This abundance and widespread use make mobile devices an appealing target for attackers. Targeting is not new but the real challenge comes from security teams not having full control over devices. Bring your own device (BYOD) policies are common but these policies often do not include internal control or management.

Often, security teams are only able to control what happens with these devices within the network perimeter. Devices may be out of date, already infected with malware, or have insufficient protections. The only way security teams may have to block these threats is to refuse connectivity which isn't practical.

The complexity of cloud environment – With businesses moving to cloud resources daily, many environments are growing more complex. This is particularly true in the case of hybrid and multi-cloud environments, which require extensive monitoring and integration.

With every cloud service and resource that is included in an environment, the number of endpoints and the chances for misconfiguration increase. Additionally, since resources are in the cloud, most if not all endpoints are Internet-facing, granting access to attackers on a global scale. To secure these environments, cybersecurity teams need advanced, centralized tooling and often more resources. This includes resources for 24/7 protection and monitoring since resources are running and potentially vulnerable even when the workday is over.

Sophisticated phishing exploits – Phishing is an old but still common tactic used by attackers to gain sensitive data, including credentials and financial information. In the past, phishing emails were vague, often posing as authority figures with wide user bases. For example, Facebook or Netflix. Now, however, phishing often leverages social engineering.

Many people willingly make large amounts of information about themselves public, including where they live and work, their hobbies, and their brand loyalties. Attackers can use this information to send targeted messages, increasing the likelihood that users will fall for their tricks.

State-sponsored attacks – As more of the world moves to the digital realm, the number of large-scale and state-sponsored attacks are increasing. Networks of hackers can now be leveraged and bought by opposing nation states and interest groups to cripple governmental and organizational systems.

For some of these attacks, the results are readily apparent. For example, numerous attacks have been identified that involved tampering with elections. Others, however, may go unnoticed, silently gathering sensitive information, such as military strategies or business intelligence. In either case, the resources funding these attacks enables criminals to use advanced and distributed strategies that are difficult to detect and prevent.

For some of these attacks, the results are readily apparent. For example, numerous attacks have been identified that involved tampering with elections. Others, however, may go unnoticed, silently gathering sensitive information, such as military strategies or business intelligence. In either case, the resources funding these attacks enables criminals to use advanced and distributed strategies that are difficult to detect and prevent.

Short review:-

Malware:-

- The total malware infection have been on the rise for the last 8 year:-
  - 2011 – 48.17 million
  - 2012 – 82.62 million
  - 2013 – 165.81 million
  - 2014 – 308.96 million
  - 2015 – 452.93 million
  - 2016 – 580.40 million
  - 2017 – 702.06 million
  - 2018 – 812.67 million
- 92% of malware is delivered by email.[4]

Phishing:-

- 56% of IT decision makers say targeted phishing attacks are their top security threat.[5]
- 83% of global infosec respondents experienced phishing attacks in 2018, an increase from 76% in 2017.[5]
- Business email compromise (BEC) scams cost organizations $676 million in 2017.[5]
- 30% of phishing messages get opened by targeted users and 12% of those users click on the malicious attachment or link.[5]
- Only 3% of targeted users report malicious emails to management.[5]
- 53% of IT and security professionals say they have experienced a targeted phishing attack in 2017.
- 50% of phishing sites now using HTTPS.[5]
- The most common malicious attachment types:
    - Office 38%, PDF 14% , XML/HTML/JS 1% [5]
- By the end of 2017, the average user was receiving 16 phishing emails per month.[5]
- 66% of malware is installed via malicious email attachments.[5]
- 49% of non-point-of-sale malware was installed via malicious email.[5]
- 30% of phishing messages were opened in 2016 – up from 23% in the 2015 report.[5]

Denial of service attack

• The first documented DoS-style attack occurred during the week of February 7, 2000, when a 15-year-old Canadian hacker, orchestrated a series of DoS attacks against several e-commerce sites, including Amazon and e Bay.[6]

• The biggest DDoS attack to date took place in September of 2017. The attack targeted Google services and reached a size of 2.54 Tbps. Google Cloud disclosed the attack in October 2020. The attackers sent spoofed packets to 180,000 web servers, which in turn sent responses to Google.[7]

SQL Injection

1998

• The SQL injection exploit was first documented in 1998 by cybersecurity researcher and hacker Jeff Forristal. His findings were published in the long running hacker zine Phrack.[8]

• In May 2020, a New Yorker was charged for hacking into e-commerce websites with the motive to steal credit card information. It was reported that the hacker along with its gang used SQL injection techniques for hacking into vulnerable e-commerce websites to steal payment card data.[9]

Zero day exfoliate

Attack On Microsoft Windows, June 2019

• The attack on Microsoft Windows that has targeted Eastern Europe was identified by a group of researchers from ESET in June 2019. The attack was regarding the local escalation privileges that were a vulnerable part of Microsoft Windows.[10]

Advance persistence threat

• Advanced persistent threats have been detected since the early 2000s, and they date back as far as 2003 when China-based hackers ran the Titan Rain campaign against U.S. government targets in an attempt to steal sensitive state secrets. [11]

• The term "advanced persistent threat" has been cited as originating from the United States Air Force in 2006 with Colonel Greg Rattray cited as the individual who coined the term. The Stuxnet computer worm, which targeted the computer hardware of Iran's nuclear program, is one example of an APT attack.[12]

Ransomware attack

- Ransomware attacks worldwide rose 350% in 2018.[13]
- Ransomware attacks are estimated to cost $6 trillion annually by 2021.[13]
- 81% of cyber security experts believe there will be more ransomware attacks than ever in 2019.[13]
- 75% of companies infected with ransomware were running up-to-date endpoint protection.[13]
- Ransomware costs businesses more than $75 billion per year.[13]
- The average cost of a ransomware attack on businesses was $133,000.[13]
- More than 50% of ransoms were paid by bitcoin in 2018.[13]

DNS attack

The Mirai Dyn DDoS Attack in 2016

• On October 21, 2016, Dyn, a major domain name service (DNS) provider, was assaulted by a one terabit per second traffic flood that then became the new record for a DDoS attack.[14]

• The first documented DoS-style attack occurred during the week of February 7, 2000, when a 15-year-old Canadian hacker, orchestrated a series of DoS attacks against several e-commerce sites, including Amazon and eBay.[15]

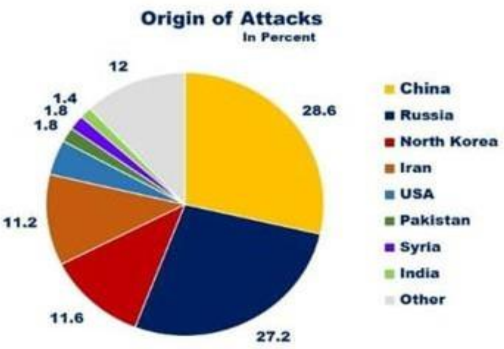
Social engineering attack

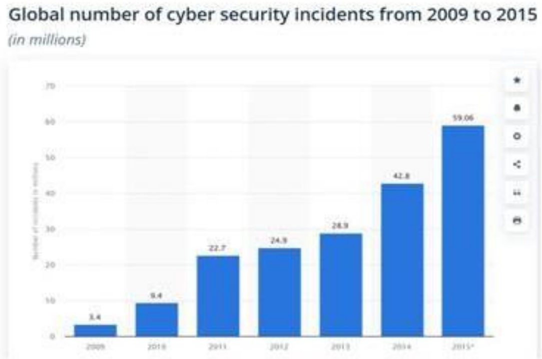
- 98% of cyber attacks rely on social engineering.
- 43% of the IT professionals said they had been targeted by social engineering schemes in the last year.
- 21% of current or former employees use social engineering to gain a financial advantage, for revenge, out of curiosity or for fun.
- Numbers of records breached by industry in 2018:
  - Social media: 2.5 billion records, or 56%
  - Government: 1.2 billion records, or 27%

- ○ Other industries: 380 million records, or 8%
- ○ Technology: 171 million records, or 4% [16]

July 22, 2019

• NEW DELHI: The home ministry has cautioned government officers against online 'social engineering' attacks seeking unauthorised access to sensitive information by impersonation via telephone or email.[17]





Cyber Security – Growing Career Opportunity

Future Scope:-

The demand for cybersecurity is at an all-time high as the global business environment shifts to cloud data storage and online management. With increased internet exposure, commercial organisational data and the personal data of users are at a threat of being misused. This has increased the demand for people in cybersecurity that are familiar with and are skilled in cybersecurity.

One of the main reasons for the industry's quick growth is the ever-changing technological landscape, which necessitates hiring bright people with varying levels of knowledge. While there are plenty of opportunities in cybersecurity, there is a scarcity of qualified candidates to fill them, as this field requires specialised expertise that is normally taught in Master's Degrees in Cyber Security.

According to the Data Security Council of India (DSCI), which is one of the top associations for cybersecurity, the cyber security business employed around 2 lakh workers in 2020, up from 1.10 lakh in 2019, and there are approximately 50,000 employment openings in the cyber security sector in India today. DSCI has predicted that the cybersecurity market will employ around 10 lakh employees by 2025.[18]

The demand for cyber security is expected to rise as digital transactions, and payments, become more prevalent, according to the DSCI. As a result, the demand for digital experts to handle the load will increase dramatically.

Conclusion:-

In this review paper the major points discovered are the different threats in cyber world and different attack Which had been taken place in the past with some sort of solution. Moreover one major issue is most of the People don't have idea about all these things and they get trapped . Now a day Use of online application get increased and cyber threats get increased too. So we have to increased the security and we have to work on the minimization of the issues (different threats people used to face now a days).

Reference:-

[1] purplesec.us/resources/cyber-security-statistics/

[2] https://en.m.wikipedia.org/wiki/cyber_threat

[3] purplesec.us/resources/cyber-security-statistics/

[4] purplesec.us/resources/cyber-security-statistics/

[5] purplesec.us/resources/cyber-security-statistics/

[6] https://www.britannica.com/technology/denial-of-service-attack

[7] https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/

[8] https://www.malwarebytes.com/sqlinjection#:~:text=The%20SQL%20injection%20exploit%20was,long%20running%20hacker%20zine%20Phr ack

[9] https://www.kratikal.com/blog/sql-injection-attack-a-major-application-securitythreat/#:~:text=In%20May%202020%2C%20a%20New,to%20steal%20payment%20card%20data

[10] https://www.phishprotection.com/content/zero-day-protection/recent-zero-day-attacks/

[11] https://www.techtarget.com/searchsecurity/definition/advanced-persistent-threatAPT#:~:text=Advanced%20persistent%20threats%20have%20been,to%20steal%20sensitive%20state%20secrets

[12] https://en.m.wikipedia.org/wiki/Advanced_persistent_threat

[13] purplesec.us/resources/cyber-security-statistics/

[14] https://www.a10networks.com/blog/5-most-famousddosattacks/#:~:text=The%20Mirai%20Dyn%20DDoS%20Attack%20in%202016&text=On%20October%2021%2C%202016%2C%20Dyn,record%20for%20a%20DDoS %20attack

[15] purplesec.us/resources/cyber-security-statistics/

[16] https://gamingsection.net/news/how-long-do-ddos-attacks-last-2/

[17] https://www.tessian.com/blog/examples-of-social-engineeringattacks/#:~:text=In%20late%202020%2C%20a%20novel,asking%20the%20person%20to%20collaborate

[18] https://www.jaroeducation.com/blog/what-is-the-scope-of-cyber-security-in-2022/amp/