Cyber Attacks and Its Types

Mintu Patel[1], Needa Mugut[2], Rahul Agarwal[3], Shubham Telkar[4],Sneha Ambore[5]
[1234]*B.Tech: Cloud Technology and Cyber Security,School of engineering Ajeenkya DY Patil University, Pune*
[5]*Assistant Professor,School of Engineering,, Ajeenkya DY Patil University, Pune*

Abstract- A cyber-attack is cautions abuse of laptop and computer systems, technology-dependent enterprises and networks. Cyber-attacks use payloads to change coding system, logic or knowledge, leading to troubled consequences that compromise may knowledge and cause cybercrimes, like data breach and fraud. Understanding attack models give additional insight into network vulnerability; that successively will be wont to defendthe system from upcoming attacksit's conjointly necessary to grasp the various forms of attack that are performed to breach the safety to interrupt down independent agency triad. This paper reveals various types of attacks and it's preventions to tackle the cyber-crime.

Keywords- cyber-attacks, types of cyber-attacks, prevention of cyber-attacks, cybercrime.

I. INTRODUCTION

Cybersecurity starts and is originated from Central Intelligence Agency triad which incorporates cybersecurity that starts with authorization, unremarkably with a username and a password. Whereas cyber-attacks are the exploitation of confidential knowledge or obtaining access over and system illicitly. Everyone is connected to web from office to home. Being connected doesn't solely concern with the advancement in life or business, it comes with the variety of potential danger like got taken valuable knowledge, lost privacy or identity, device infected by malware and lots of additional. On a day to day basis true is obtaining worse within the cyber world. Security for any legitimate network is below threat of attack. There is an increase in the range of varieties of attacks additionally since the last decades, cyber-attacks are evolving into new varieties day by day, a number of the researchers have defined these cyber-attacks as cyberwar.

Most of the cyber-attacks are not detected by the organization and if it detected they don't have any reaction plan to tackle the situation. [10][11]Some latest survey shows that the globally 68% and in India 76% hits by online attacks. Some of the common cyber-attacks and its definition are as follows:

II. CLASSIFICATION: TYPES OF ATTACKS

1. Password attack
2. SQL injection attack
3. Cross-site scripting (XSS) attack
4. Eavesdropping attack
5. Malware attack
6. Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks:
7. Man-in-the-middle (MiM) attack

a. Definition:

1. Password attack:

Passwords are the basic elements of authentication of any account of for maintaining confidentiality. Cracking a password is a kind of attack in which a non-legitimate user get access to the account or confidential documents. In simple terms, password attack means to get access over the password or knowing some person password by a non-legitimate user by using techniques such as social engineering, phishing and many more e.g.: Brute-force, dictionary attack.

2. SQL injection attack:

SQL injection attacks have become a common threat to database-driven websites. SQL injection attack is mainly a code injection formula or method, in which harmful SQL statements are fired into an entry field for executing it and getting access over that database by an intruder.

Ex: code injection, log injection, XML injection, etc.

3. Cross-site scripting (XSS) attack

This kind of attackis performed by injecting malicious XSS code in the websites as end users has no way to detect, they assumed it as it came from a trusted source.

It can be further classified in types: -

A. Reflected XSS attack: In thisattack, the inputs given by the user reflected back to the user.

B. Stored XSS attack: In this attacks, the malicious code is stored in its databases and can access any time remotely.

4. Eavesdropping attack

This kind of attack, occurs through hijacking the sessions over the networks. By eavesdropping, an intruder can get credentials or confidential information that a user transmitting over the network.

Eavesdropping can be either passive or active:

a. Passive eavesdropping: In this eavesdropping, the message transmission in a network is been captured by the hacker to get the information from it.

b. Active eavesdropping: In this eavesdropping, a hacker actively grabs the information by pretending himself as a

friendly unit and by sending queries to transmitters. This is called tampering. Detecting the active eavesdropping is an additional task than passive eavesdropping as one has to find passive before.

5. Malware

Malicious software can be defined as an unwanted package which is loaded to one's system with required content. It can combine itself with the original code and expand. It can be hidden in useable applications or duplicate itself across the Internet.

A. Types of malware:

5.1.1**Viruses:** A virus is a self-replicating malicious computer program that replicates by creating copies of itself into a mother computer program when executed. It can be also executing an instruction that can cause harm to the system. It waits for an event to get a trigger.

B. **Worms:** A worm is a self-replicating malicious computer program that replicates by creating copies of itself and spread in networks and harm it in many ways. It may or may not change the system behaviour. Depended on the code it gets executed.

C. **Trojan Horses:** It pretends to be a normal application, and generally spread with a form of social engineering. This attack consists of payload which loaded to the victim's system by social engineering.

6. Denial of service (DOS) Attack: In this kind of attack ,Hackers makes an attempt to make a server unavailable to the legitimate user. This is normally done with flooding the server with number of request. Dos uses the single server and the single network to attack a server. Distributed Dos (DDoS) uses multiple systems and internet connection to flood a server with requests, making it harder to counteract.

a. Dos can be identified into:

b. **Volume Based Attack:** In this attack, aim is to fill the bandwidth of the attacker site, and calculated in bits per second.

c. **Protocol Attacks:** In this attack, the consumers' actual server resource is made unavailable.

d. **Application layer Attacks:** The goal of this attack is to break into the web server.

7. MAN-IN-MIDDLE (MIM) ATTACK: In this kind of attack the attackers intercept the connection between a client and the server and acts as the bridge between them leading the attacker to enter and change the data in the intercepted communication.

III. LITERATURE REVIEW

[1] Mohan V Pawar, "Network security and types of network attacks". This paper focuses on various types of attacks which help to categorized various types of attacks based on networks.

[2] Lucas Oliveira Batista1" Fuzzy neural networks to create an expert system for detecting attacks by SQL Injection." Reference of this paper result in deep studying of SQL injection and help to find the preventions.

[3] "Hamad AL-Mohammadi ", Cyber-Attack Modeling Analysis Techniques: An

Overview. The following paper demonstrated three techniques which help to understand the cyber -attack and reveal the vulnerabilities of the system and also by analyzing the data one can find the pattern of attacks."

[4] Ruzaina khan", Network threats, attacks and security measures: a review

The respected authors explain various types of attacks with analysis along with preventions like intrusion detection system (IDS), firewalls and anti-viruses system.

IV. ANALYSIS

As there is an increase in cyber-attack the analysis of different reports is being gathered together as follows:-

- One of the surveys shows that out of 1,300 IT organization, 56% of them identified targeted phishing attacks has emerged as their biggest current cybersecurity threat.
- Around 76% of businesses have being a victimizedby phishing attack in the previous year.
- Kaspersky's Anti-Phishing system was triggered 246,231,645 times in 2017.
- According to the study performed by Sophos,75% of organizations infected with ransomware with updated security system.
- The global damage costs connected with ransomware attacks is estimated to reach $11.5 billion in 2019 according to the statistical data of cybersecurity ventures and estimated there will be a ransomware attack on businesses every fourteen seconds by the tip of 2019, up from every 40 seconds in 2016.
- This doesn't embody attacks on people, that happens even additional often than businesses

This points of the report specified that phishing and ransomware are widely used cyber-attacks.

Taking a view on attack and data breach are:-

Here are some key t stats from the Ponemon Institute's 2018 value of a knowledge Breach 2018 study for IBM.

• The average cost of the data breach to companies globally is around $3.86 million (U.S. dollars).

• The average time it was taken by an organization to detect a data breach is around196 days

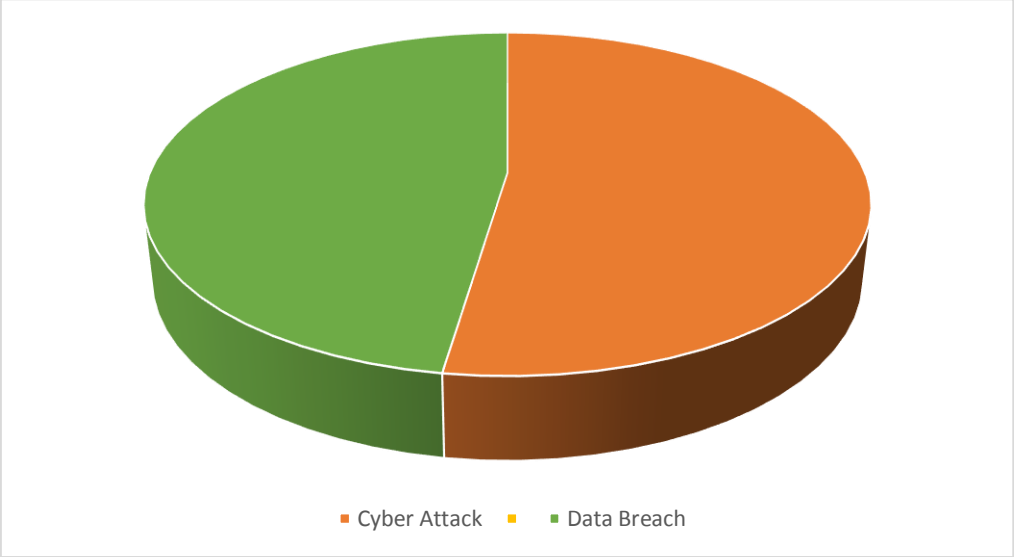

Fig.1: This pie chart shows the number of cyber-attacks and the data breached level

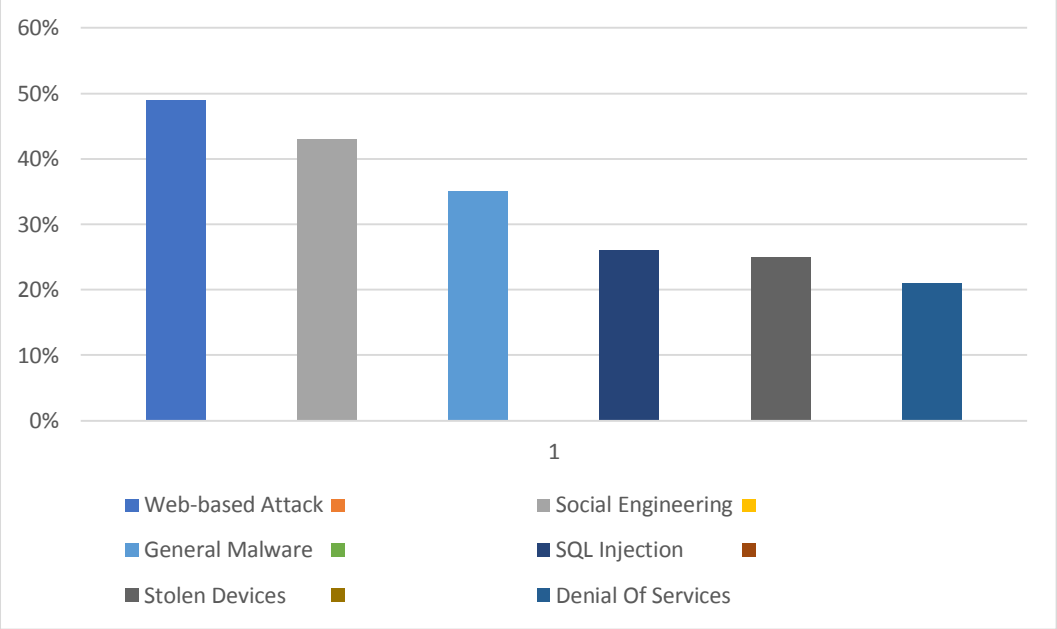

Fig.2: This bar graph shows that the intensity of cyber-attacks performed

a. Top 8 cybersecurity statistical facts

• Organization gets infected by receiving around 92% malware by email.

• 77% of compromised attacks in 2017 were severe attack and cost a lot of damages.

• The average ransomware attack costs a company $5 million.

• 88% of companies invest more than $1 million on preparing for the General Data Protection Regulation (GDPR).

• Standalone security department is present in 25% organization.

• An industrial control system security accident is experienced by 54% of companies.

• An IoT security occurrence is experienced by 61% of companies.

b. Cybersecurity Facts

- According to SC Media, The number of passwords used by humans and machines worldwide is likely to touch 300 billion in 2020.
- According to Small Business Trends, 43% attacks are targeted to small business.
- According to Panda Security, around 230,000 new malware samples are created and its rate is growing.
- According to Vanson Bourne, 90% of hackers cover their tracks by using encryption.
- According to Computer World, most targeted operating system are windows and android.
- According to Quick Heal, In Between January and May 2018, there were over 3 million crypto jacking hits.

c. Cybersecurity Costs

- According to Accenture, Information loss is the most expensive components cyber attacks with 43% of total loss.
- According to CyberSecurity Ventures, will have been harm around 6$ trillion annually by 2021.
- According to Accenture, The malware and web-based atttacks emerged as top kind of attack.

d. Previous Data :

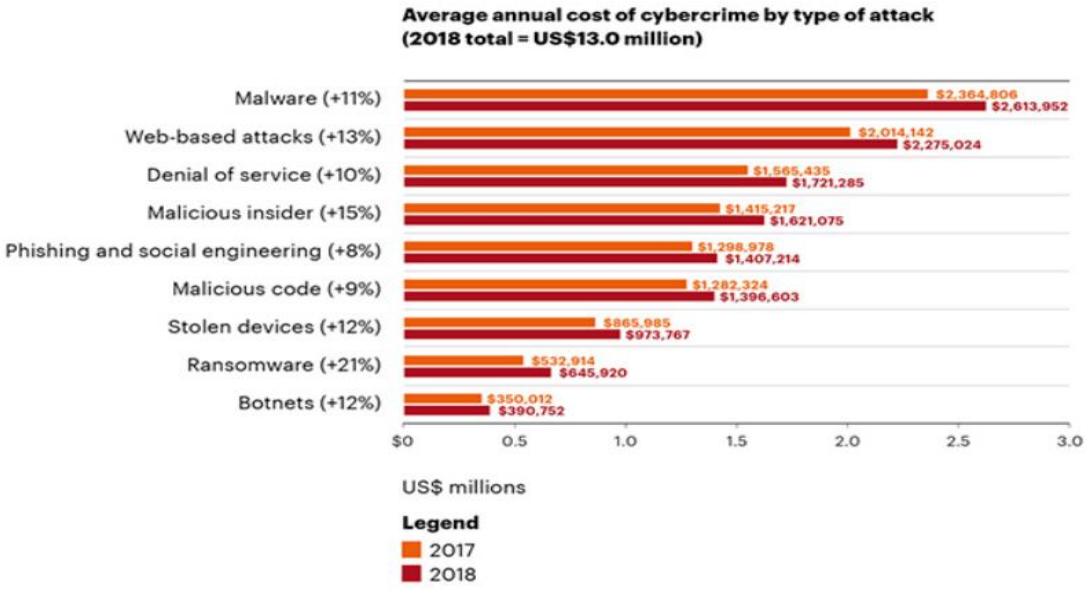

Fig.3: The average annual cost of cybercrime by type of attacks.

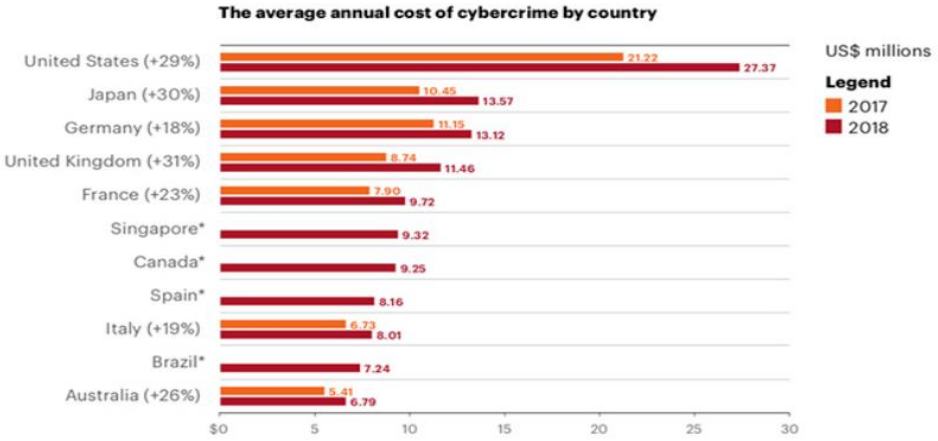

Fig.4: The average cost of cybercrime by country

V. PREVENTION

- Back up files, consistently
- Update Everything
- Stop malware when it Starts
- Encryption of Data
- Validation
- Choose a highly secured firewall that provides best threat protection till date
- Educating Users
- Employ or consult cybersecurity Experts
- Intrusion Detection Systems

VI. CONCLUSION

Security act as backbone in any field and it is the same for the digital world. There is no system to grant 100% security but there is a way to achieve the security goals by various policies. To defend from intruder one should first define a what security means to them.On the basis of that security definition cyber expert lay the foundation of the secured wall of the organization. For best security expert must well focus on every possible way of the attack and ready with a reaction. In this paper, Authors try to analyze the size of damage can be occurred and most types of attack are faced in the digital world. Also, try to convey to that don't get trapped in social engineering as it reveals many ways for the intruders. The organization should also spend money on such awareness rather than on physical assets.

VII. REFERENCE

[1]. Mohan V Pawar, "Network security and types of network attacks".

[2]. Monali S Gaigole, "Study of network security with its penetrating attacks".

[3]. Neha Khandelwal, Prabhakar. Kuldeep Sharma, "An Overview of Security Problems in MANET".

[4]. Ali Ghaffari, "Vulnerability and Security of Mobile Ad hoc Networks".

[5]. A White Paper, ―Securing the Intelligent Network‖, powered by Intel Corporation.

[6]. Mohammed Nasser Al-Mhiqani, "Cyber-Security Incidents: A Review Cases in Cyber-Physical Systems"

[7]. Lucas Oliveira Batista1," Fuzzy neural networks to create an expert system for detecting attacks by SQL Injection. "

[8]. Hamad AL-Mohannadi, "Cyber-Attack Modeling Analysis Techniques: An Overview"

[9]. Ruzaina khan, "Network threats, attacks and security measures: a review "

[10]. https://us.norton.com/internetsecurity-emerging-threats-10-facts-about-todays-cybersecurity-landscape-that-you-should-know.html

[11]. https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

[12]. https://secure2.sophos.com/en-us/security-news-trends/whitepapers/gated-wp/uncomfortable-truths-of-endpoint-security.aspx