How to Cite:
Sharma, A., Tyagi, A., & Bhardwaj, M. (2022). Analysis of techniques and attacking pattern in cyber security approach: A survey. *International Journal of Health Sciences*, *6*(S2), 13779–13798. https://doi.org/10.53730/ijhs.v6nS2.8625

Analysis of techniques and attacking pattern in cyber security approach: A survey

Aman Sharma
Department of Computer Science and Information Technology, KIET Group of Institutions, Delhi-NCR, Muradnagar, India

Anushka Tyagi
Department of Computer Science and Information Technology, KIET Group of Institutions, Delhi-NCR, Muradnagar, India

Dr. Manish Bhardwaj
Department of Computer Science and Engineering, KIET Group of Institutions, Delhi-NCR, Muradnagar, India

***Abstract*---**IT or Cybersecurity. It's the protection of computer systems and networks against data leakage, theft or damage to their hardware and software as well as service interruption or misdirection. Increasing reliance on computer systems, such as smart phones, televisions and the micro devices that make up the Internet of Things, has made this field increasingly vital. Data security has risen to the top of the to-do list in today's globe. Cybercrime is being tackled in a variety of ways by governments and corporations around the world. There is still a lot of anxiety about cyber security, despite several efforts. This Paper provides an Intensive survey of various cyber-attacks in India and their Countermeasures.

***Keywords*---**cyber security, cyber attacks, cybercrimes, cyber solutions.

Introduction

We all live in a fast-paced and developing society, and the Internet is now the most important infrastructure in our daily lives. Our data is our most valuable asset or liability on the Internet. It may be our credit card information, medical records, financial transaction reports, military secrets, business strategies, chats, videos, and anything else. What happens if the evil people get their hands on it? When it comes to protecting our data from unauthorised access and modification, this is where cybersecurity comes into play.

Cybersecurity is needed today because of the loopholes we missed when constructing some of the most advanced systems in the world. As long as there are loopholes, there are always going to be people exploiting new technologies for their own gain. In the same way that we can forget to install a lock or security system on the main door of a house that we have built, this situation is analogous. According to Statista, Eastern Asia and nations in which India has ranked second in terms of Internet users (in millions) will have the most Internet users in 2021. The numbers are represented in the following graph by various demographic groups.

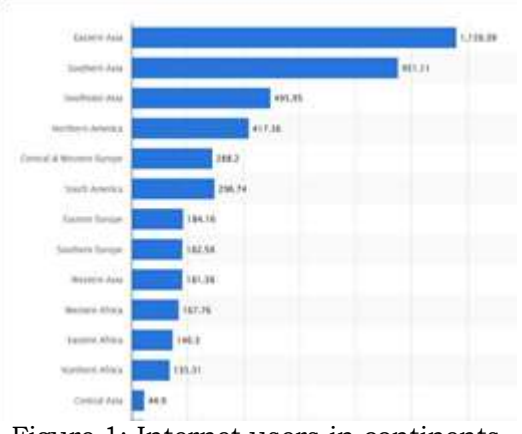

Figure 1: Internet users in continents

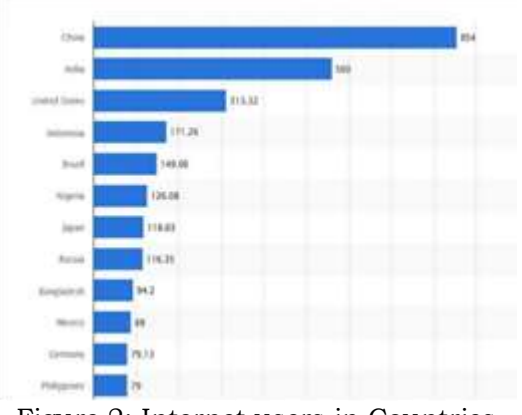

Figure 2: Internet users in Countries

People, corporations, and the government all generate enormous amounts of data as a result of the widespread adoption of mobile phones, laptops, and other electronic devices. These days, we do almost everything via the internet, including the exchange of personal information and money. That has given the criminals a chance, too. Businesses in India could lose more than 1.25 lakh crore to ransomware, malware, and other security breaches in 2020, according to an estimate. Consequently, the relevance of cybersecurity is being recognised by a growing number of people. In India, which exports software and services worth $150 billion annually, a torrent of eager, imaginative start-ups in the

cybersecurity field are tackling this global dilemma. Global Capability Centers and 230 start-ups in the cybersecurity area collectively produced $11 billion in revenue last year, according to the Data Security Council of India (DSCI), the industry's main body. This source of income is increasing at a CAGR of 27%. With the abundance of engineering talent in India, India and its enterprises have the potential to become global leaders.

Literature Review

According to Statista[1], In 2020, India saw a significant increase in the number of cyber-crimes reported. More than 50,000 incidents of cybercrime were reported in 2013. It was Karnataka and Uttar Pradesh that accounted for the most of the time. In comparison among the two, Uttar Pradesh had the highest number of cybercrimes, with over 6,000 cases reported to authorities in 2018. Karnataka, India's tech state, followed suit in 2013. Most of these cases were filed under the IT Act with the intention of defrauding or sexually exploiting victims. Consumers in India are thought to have lost over $18 billion in 2017 as a result of cybercrime. But these were based only on the numbers that had been reported. Due to lack of cyber-crime awareness or mechanisms to classify these crimes in India, it is highly likely that the actual figures will be under-reported.

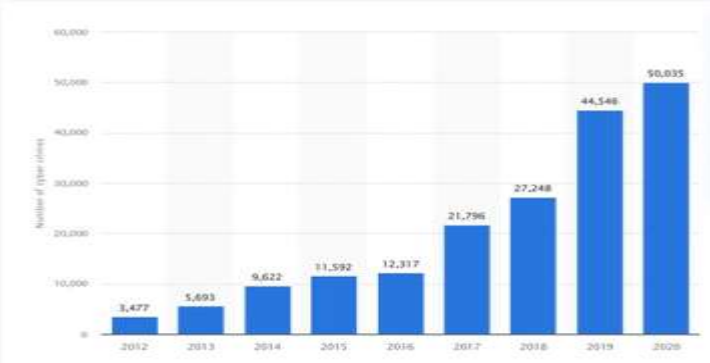

Figure 3: Number of cyber-crimes reported across India from 2012 to 2020
Source(Statista)

According to *Pintu Shah [2]*, In India, a large percentage of people use their smartphone as their first computing device . Users in other countries who have gone through the learning curve of dealing with malware on other Internet-enabled devices like laptops and desktops have more experience dealing with Internet-enabled devices and, as a result, has less knowledge of how to deal with security threats like malware. Consequently, the inexperienced Indian smartphone user may be more vulnerable to Internet security breaches than the citizens of developed economies. In accordance with Pintu Shah's findings, In general, the people who took the survey didn't behave securely. Screen locks and fingerprint scanners are among the most popular smartphone security features adopted by respondents. Technical security controls like encryption and remote wipe have yet to be adopted by respondents or they are unaware of them. Gender, age, mobile OS, and mother tongue were found to have statistically significant correlations with cybersecurity behaviour and practices. Most people are

motivated to keep their device and data safe, but they are only moderately aware of threats or able to do anything about it. As a result, in order to keep our citizens safe, it is critical that we have a thorough understanding of hacking techniques, vulnerabilities, and methods.

According to Suman Acharya, Sujata Joshi[3] There are a lot of people in the banking and financial sector (BFSI) industry, and they're all over the world. Over the past few decades, banking services have become more accessible to the less fortunate members of society. According to the 2017 Global Findex database, there have been nearly 1.2 billion adults with bank accounts since 2011. Most Indians, according to a study, are switching to digital banking, with 51% preferring online channels and 26% using bank websites and mobile banking services. Cybersecurity has become a major issue for banks as they have become increasingly digitised. Only 22% of India's cyber-attacks occurred in the banking sector.

Related Evidences and Findings

It has been reported that 17,560, 24,768, 26,121 and 25,870 Indian websites were breached in 2018, 2019, 2020, and 2021 (till October) accordingly," Minister of State for Electronics and IT Rajeev Chandrasekhar stated in a written reply to the Lok Sabha[4]. In India, cyber-attacks have escalated to the point where our country ranks fourth in the world's most targeted countries.

1. Unacademy Data Breach : In May 2020, Unacademy, an educational technology start-up, suffered a data breach that compromised the accounts of 22 million Indian users. For sale on the dark web were the hacked accounts' email addresses, usernames, and passwords."
2. Bigbasket Data Breach : In October 2020, Big Basket's user data was put up for sale in an online cybercrime marketplace. Around 20 million Indian users' personal information was sold for $40,000. People's names, email addresses, PINs and phone numbers were among the data that was put up for sale.
3. COVID -19 Data leak : Thousands of Indian patients' COVID-19 lab test results were leaked online in January 2021, seemingly through government websites. Using Google, anyone can access the data that was leaked earlier today. Patients' birth dates, full names, testing centres, and testing dates were all included in the sensitive information.
4. Police Identities leak: At some point in February of 2021, 500,000 Indian police officers' personally identifiable information (PII) were put up for sale on a database sharing forum. Police conducted an exam on December 22, 2019, and the data was traced back to that date. In addition to the exam candidates' full names and contact information (email addresses and phone numbers), the leaked information also included their criminal histories and FIR records.
5. Upstox data Breach: Approximately 2.5 million Upstox customers were affected by the April 2021 data breach. There were more than 56 million KYC data files that included email IDs, passport numbers, personal identification numbers (PAN), and more. Infiltrating a third-party warehouse

allowed the notorious hacker collective Shiny Hunters access to the KYC details and contact information.

6. IIM JOBS Data leak: The data of 1.4 million Indian job seekers was leaked online in November 2020 after a cyber-attack on the IIMjobs job portal. The victims' names, email addresses, phone numbers, precise location, links to their LinkedIn profiles, and their industry of work were among the data that was accessed by the attacker.
7. Mewat : Located on the Haryana-Uttar Pradesh border, Mewat is close to Bharatpur, Alwar, and Bhiwandi in Rajasthan, as well as Mathura, Uttar Pradesh. It has sounded the alarm after reporting 70% of the most recent cases of Cyber Fraud. Known for phishing calls, Mewat is also notorious for exploiting other verticals, such as banking, social media profiles and online marketplaces, in order to gain access to personal information. These robberies have been reported by nearly every person in the villages of Alwar and Bharatpur, including Ramgarh, Govindgarh, Naugava, and Bhiwandi in Alwar Rajasthan. Robbers are typically between the ages of 18 and 28. 70 percent of the robbers were tracked down in Mewat's Alwar and Bharatpur regions.
8. Jamtara : According to the Indian state of Jharkhand, Jamtara is home to a city as well as a designated notified area in the Jamtara Sadar subdivision of the larger district. As a result, it has earned the moniker "India's phishing capital" As a result of numerous phishing incidents that took place across the country, it was given this name. It was reported that Indian police from 12 different states visited Jamtara on 23 separate occasions between April 2015 and March 2017. According to some estimates, one of the most underdeveloped districts was responsible for 80% of all cybercrimes. Involved parties purchased high-end SUVs and built extravagant bungalows next to dilapidated cottages in the same neighbourhood.

This list could go on indefinitely, but the point is to raise awareness about the seriousness of India's vulnerability to cyberattacks and the urgency of finding a long-term solution.

Common Types of Cyber Attacks

Phishing

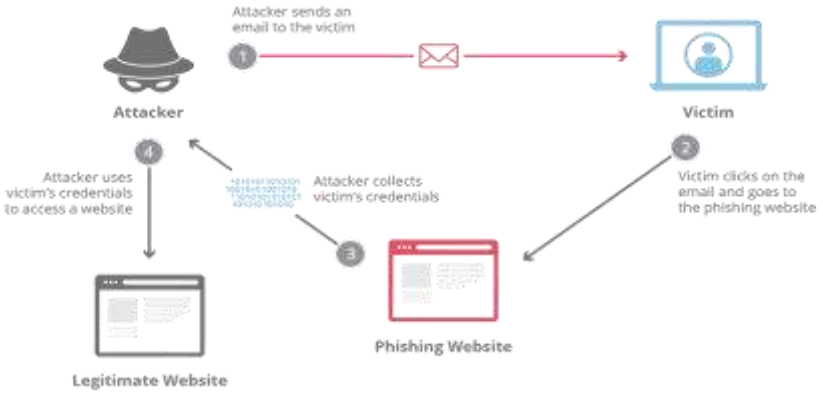

Figure 4 : Circuit of a Phishing Attack

Sending falsified emails that appear to come from a trusted source is known as "phishing." Email or other communication that is designed to entice a victim is the first step in the process of phishing The sender's identity is obscured so that the message appears to come from a well-known source. Often, the victim is tricked into disclosing personal information on a scam website after falling for the ruse. Malware can also be downloaded onto the target's system from a third-party source. Figure 4 shows an example of one of these types of mail.

Figure 5: A Sample Fraudulent Phishing Mail

Phishing in India

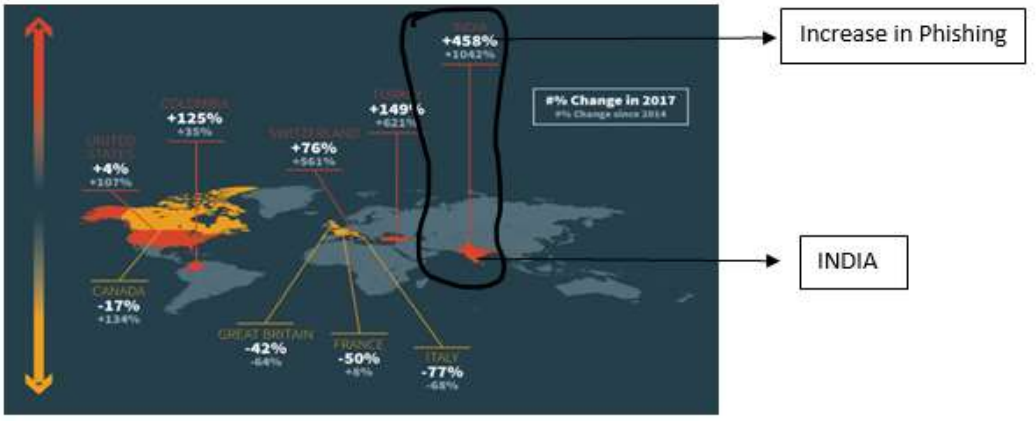

Figure 6: Increased Phishing Rates in India

During the pandemic, phishing attacks targeting organisations increased significantly because millions of employees working from home became a primary target. According to a report by UK-based cybersecurity firm Sophos [6], a large majority (83 percent) of Indian IT teams reported an increase in the number of phishing emails targeting their employees in 2020. Phishing attacks can be viewed as a low-level threat by organisations, but this underestimates their power. To begin an attack, phishing is often the first step.

Business Insider India[7] has a news report on this. Phishing attacks via WhatsApp and Telegram are on the rise in India, according to a new report. "Phishing in instant messaging apps is still a popular method of scamming, according to statistics. One reason is that these apps are so popular with the

public, and because they have built-in functionality that can be used to carry out attacks "According to Kaspersky's Tatyana Shcherbakova, a senior web content analyst.

The difference between a phishing attack and something else can be as small as a single character or a typographical error. According to a new report from the Cyber Cell Unit Delhi[8], the sender of a phishing attack typically asks for assistance in facilitating the transfer of a large sum of money via email. As a reward, the sender typically offers a commission in the millions of dollars. Money is then requested to cover some of the costs associated with the transfer from the scammers' side. As soon as the scammers receive the money, they will attempt to get more money by claiming that the transfer is having problems. In such matters the victims normally allege that they have received emails from unknown sources wherein they have been informed that:

- Either they've won a multi-million dollar lottery prize; or
- For the transfer of illegal funds from a country in Africa, their assistance is required ; or
- Somewhere in Europe or the United States, they've been given the opportunity to work in a hotel.; or
- Throwaway prices are advertised for products ; or
- An email may be sent from the victim's email account to all of her contacts, requesting money for a perilous situation; in some cases, the victim's address book in her emailing list is compromised.

The victims are tricked into parting with large sums of money, either as money transfer fees, taxes, or transportation costs, over a period of time. The victims, it appears, are the recipients of spam emails, which they promptly reply to, and as a result, they wind up paying money to anonymous parties for purposes that never existed. In most cases, these crimes are committed from abroad. Either offshore accounts or Indian courier accounts are used to store the funds.

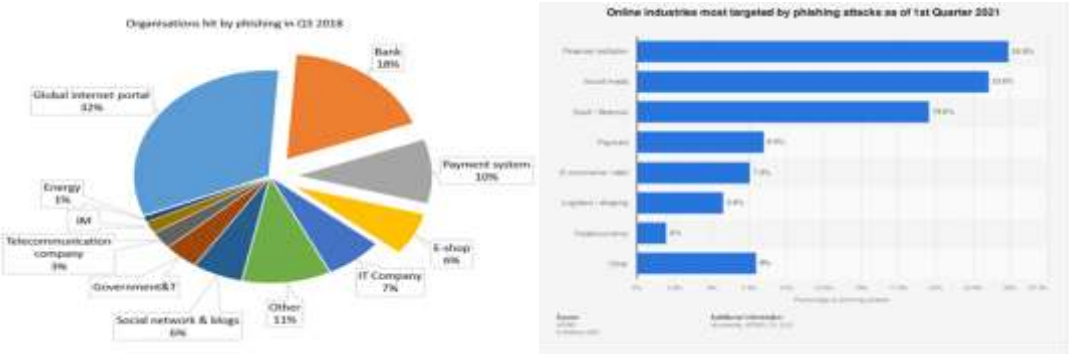

Figure 7: Distribution of sectors Effected by Phishing Attacks

This Attack has a lot more areas to be discovered, Author have mentioned only few of its characteristics Based on his Research And Developments, for more information, one can refer Internet.

Man-In-The-Middle Attack

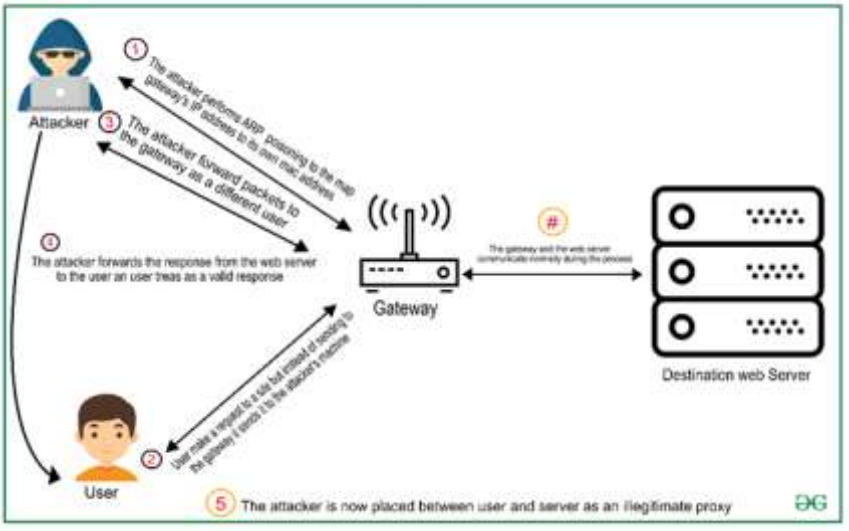

Figure 8: Basic Diagram of MitM Attack

MitM attacks, also known as eavesdropping attacks, can occur when an attacker gets into the middle of a two-party transaction and steals information from both parties. Filtering and stealing data are possible once the traffic is disrupted by the attackers. A cyber-attack like this one occurs when the attacker acts as an intermediary between the parties involved. In order to make both parties feel as if they are communicating over a secure network, it can be used.

Two common points of entry for MitM attacks

1. In public Wi-Fi that is not secure, attackers can get between a user's device and the network. The attacker gains complete access to the visitor's computer without them even realising it.
2. Malicious software can be installed on a victim's device to process all of the victim's data.

Typically, a web application consists of a client and a server. A third entity, the communication channel, is often overlooked. This can be accomplished with either a wired or a wireless connection. One or more servers may be able to forward your request to multiple servers in the most efficient manner. Servers like these are referred to as "proxies." This type of attack occurs when a third party intervenes in the network by intercepting and altering communications between clients and servers. Man-in-the-middle attacks are then labelled as a threat to the network This rogue proxy is frequently mistaken for a legitimate communication point by the other endpoint. It serves as both a server and a client, handling all of the data exchanged between the two parties.

Assume you're using a Wi-Fi network to make a purchase at your bank. While this is going on, an attacker is on the same network. The attacker takes this action:
For the attack, the attacker uses rogue ARP packets to map the access point's IP address to the attacker's device's MAC address in the system.
Caches for rogue packets exist on every network device.
It is possible to send data packets to your bank's web server by using ARP, which sends them to the access point (which is the default gateway for the network).
The attacker's computer receives the packets. As a result of this, attackers can now read and modify the requests contained in the packets before they are sent.
Since the attacker is between you and your bank's server, you are at risk of being attacked. The attacker has access to all of your server's sensitive data, including your password.
The ARP cache can be poisoned in order to launch an MITM attack.
DNS spoofing is the first.
IP spoofing is the second method.
Create a rogue Wi-Fi AP is the third method
Fourth one is SSL spoofing, and so on.
SSL can help prevent these attacks from succeeding.

To the attacker's computer, packets are sent in the same way. Even if an attacker gets their hands on the data, they will be unable to do much with it because it is encrypted and only legitimate endpoints have the key to decode it. When SSL is properly configured, it is only able to function. However, there are ways around this protection mechanism, but they are extremely difficult to carry out. Even so, an attacker can do a great deal of harm if the online application with which the user has been communicating does not use something called the nonce. For the duration of the session, the attacker has the ability to intercept the encrypted requests and then carefully resend the logging in requests.

Key concepts of Man in the Middle Attack

This attack takes use of client-server communication leaks to get access to confidential data. The data transfers that take place as a result of this attack go unnoticed. Attachments, links, and duplicate webpages are some of the tools used by the attacker in this attack. It's a type of cyber-attack in which the attacker remains between the two parties and performs its functions. One of its primary goals is to create a false sense of security by making the two parties believe they are conversing over a secure network. Performing a man-in-the-middle attack on someone else while making them believe they are chatting with each other without realising their entire communication is being controlled by someone else is an example of an MITM attack.

It is a common attack?

The Man in the Middle Attack has been rare for a long time. To target a specific individual, this type of attack is most commonly employed. This isn't your normal phishing or virus or ransomware attack.

Case Study-1: Google and Apple have removed Equifax's apps from their stores following the discovery of the data leak. Due to the lack of HTTPS, attackers were able to see all user data when they were logging into their accounts.
Case Study- 2: Hackers gained access to a significant number of certificates after breaching the security of an online certificate registrar service. Certificates issued by these organisations allowed the attacker to spoof a legitimate website in order to steal data from the user.
Case Study-3: The assailant targeted a bank as one of his victims. The attacker sends the customer an email notifying them that someone has attempted to access their bank account and requesting that they verify their information. The email sent to the consumer was a phishing scam. So, when a victim clicks on the link, they are taken to a bogus website instead. The fake website will look to be authentic. After providing the requested information, the victim will be taken back to the original website's home page. An intruder has gained access to the victim's online banking and credit card information.

Advantages: Using a public Wi-Fi network can put the user at risk of a Man in the Middle Attack. There may be false software updates that appear up if the user's connection has been hijacked by the attacker.
Disadvantages: When the victim clicks on a link or attachment, or connects to a public Wi-Fi network, they are subjected to this type of assault. To avoid the attack, the victim must not click on the anonymous links or connect to any public Wi-Fi. As a result, it is possible to avoid this attack by being more attentive.

Users should be aware of

The availability of public Wi-Fi networks. Don't connect to a Wi-Fi network whose name doesn't appear to be correct.

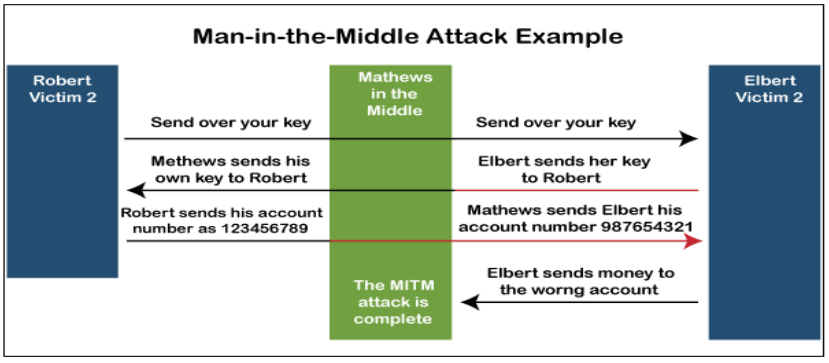

Figure 9: Example of MitM Attack

This Attack has a lot more areas to be discovered. The Author has mentioned only few of its characteristics Based on his Research And Developments. For more information, one can refer Internet.

Distributed denial-of-service attack

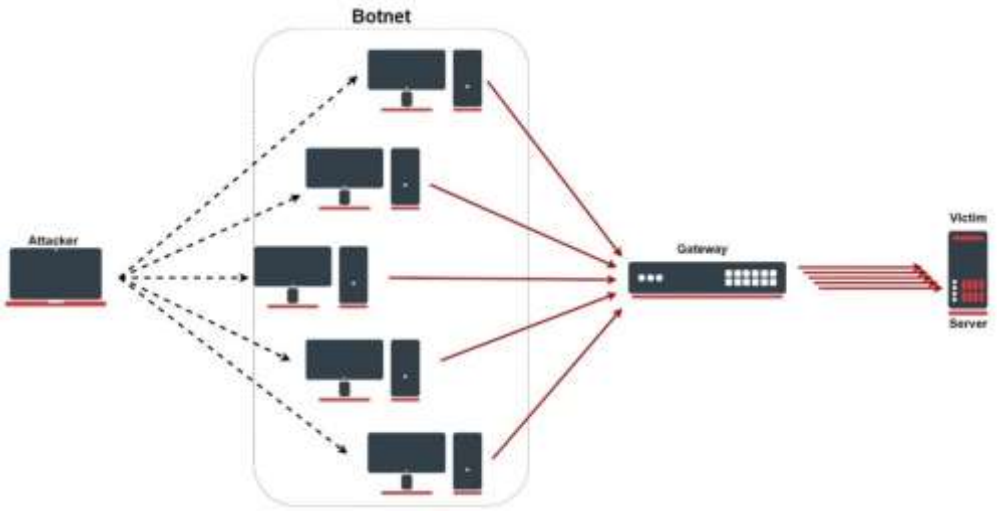

Figure 10 : Basic Diagram of DDoS Attack

In order to overwhelm a network with unnecessary traffic, attackers use distributed denial-of-service (DDoS) assaults. In the event of a DDoS assault, the network's overall performance is adversely affected, and/or essential infrastructure services are completely disrupted. This type of attack can shut down even the most popular websites, according to Sam Cook (a data journalist, privacy advocate, and cord-cutting expert). Servers crash because they can't keep up with the flood of junk requests. Recovering from these outages might take hours. Because of the sheer volume of requests these attacks generate, even the largest websites can be brought to a grinding halt. Servers crash because they can't keep up with the flood of junk requests, and it can take hours to get them up and running again.

In recent years, the frequency of DDoS assaults has significantly increased. The number of ransom DDoS attacks grew by 75% in Q4 2021 compared to the previous quarter, according to a Cloudflare analysis. During the coronavirus pandemic in Q2 of 2020, we saw a substantial and long-lasting increase in attacks. The fact that we're still witnessing a net growth in the number of people working from home and remotely is not surprising.

Cloudflare claims that

- Year-over-year, ransom DDoS attacks climbed by 29%, and quarter-over-quarter, they increased by 175%.
- The manufacturing industry saw a 641 percent increase in the number of application-layer DDoS attacks quarter-on-quarter.
- December 2021 alone saw more network-layer DDoS attacks than the entire first and second quarters of 2021 put together. Moldova has the greatest percentage of network-layer DDoS activity in the world, with attacks quadrupling quarter-on-quarter.

In 2021, there was a significant increase in DDoS activity compared to prior years. However, we've witnessed an increase in short-duration attacks, and according to Secure list, the average DDoS attack lasts under four hours. Cloudflare has confirmed these findings, reporting that most attacks last less than an hour. Automated DDoS mitigation solutions must be in place at all times. That said, several assaults lasting 10 days or more have been documented, and it appears that longer attacks are becoming the norm. More people are now aware of the dangers posed by these attacks. The number of people searching for "DDos" and "denial-of-service attack" rose sharply in June of that year. We know why: it was around this time when Amazon declared it had beaten back the largest-ever known DDoS attack.

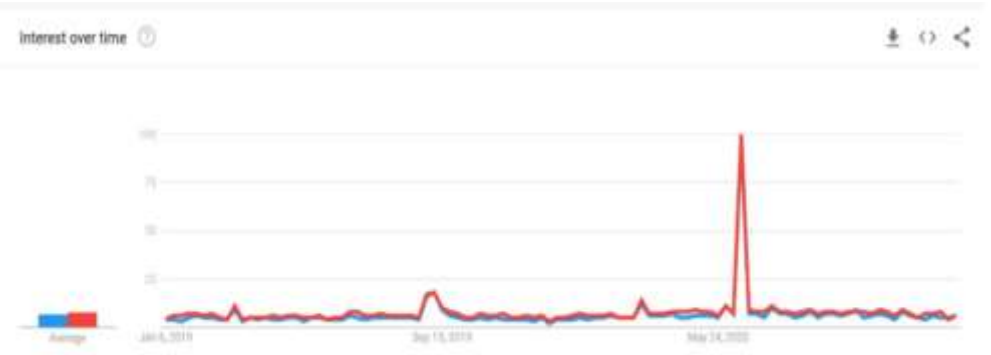

Figure 11: Search Trends of DDoS Attack

In most cases, DDoS assaults are launched from the following locations:

- China
- The US
- Korea
- Russia
- India

Figure 12: Major DDoS Attacking Countries

This Attack has a lot more areas to be discovered. The Author has mentioned only few of its characteristics Based on his Research And Developments. For more information, one can refer Internet.

SQL Injection Attack

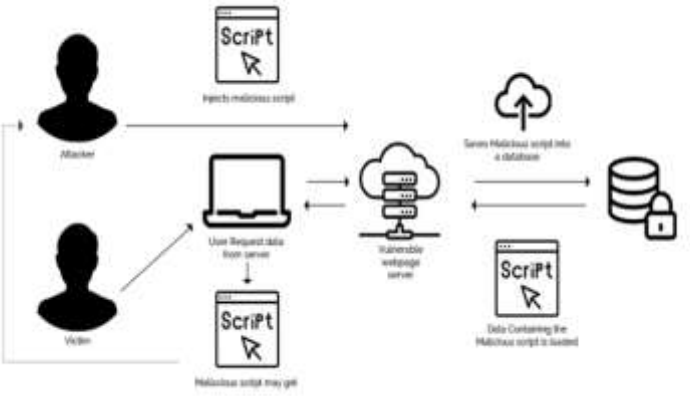

Figure 13: Basic SQL Injection Diagram

It is possible for an attacker to tamper with an online application's database queries by using SQL injection, which is a web security vulnerability. Data that would otherwise be hidden from an attacker can now be viewed. Other people's data, as well as data that the application itself can access, could be included in this category. An attacker can frequently alter or remove this data, resulting in long-lasting modifications to the app's content or behaviour. Attackers in some cases have the ability to escalate SQL injection attacks into more serious attacks, such as denial of service attacks and back-end server compromises.

What is the impact of a successful SQL injection attack?

Unauthorized access to sensitive data, such as passwords, credit card numbers, or personal information, can be the outcome of a successful SQL injection attack. SQL injection attacks have been responsible for a number of high-profile data breaches in recent years, resulting in reputational harm and regulatory fines. When an attacker gains access to a company's systems through a persistent backdoor, a long-term compromise might occur that goes unreported for an extended length of time. A vast range of SQL injection vulnerabilities, attacks, and strategies can be found in many contexts. As an example of SQL injection,

- ⇨ Retrieving data that has been concealed in a SQL query so that more relevant results can be returned.
- If you want to mess with the application's logic, you can edit a query to do so.
- UNION attacks, which allow you to access data from multiple tables in a single query.
- The database can be examined in order to learn more about its version and structure.

- The results of a query that you control are not returned in the application's answers, which is known as "blind SQL injection."

One example of this would be retrieving secret data

Assume you're using a shopping app that categorises the items you're looking at. User browsers request the following URL when they select the Gifts category:

```
https://insecure-website.com/products?category=GiftS
```

An SQL query is then executed by the programme, which retrieves product information from the database:

```
SELECT * FROM products WHERE category = 'Gifts' AND released = 1
```

The following is the SQL query's request to the database:

- all information (*)
- based on the product list
- in the Gifts category
- and the latest release is 1.

It's being used to hide products that haven't been released by setting the release limit to 1. For products that have yet to be published, presumably released = nil or (0). Because there are no safeguards in place to prevent SQL injection attacks, an attacker can launch an attack like the following:

```
https://insecure-website.com/products?category=Gifts'--
```

This leads to the following SQL statement:

```
SELECT * FROM products WHERE category = 'Gifts'--' AND released = 1
```

Using the double-dash sequence — indicates that the rest of the query is treated as a comment in SQL, which is the most important point here. Effectively removing AND released = 1, this effectively removes the rest of the query. In this case, all products are displayed, even those that have yet to be released.
To make matters worse, an attacker can make the app show all of the products in any category, even ones they aren't familiar with :

```
https://insecure-website.com/products?category=Gifts'+OR+1=1--
```

This leads to the following SQL statement:

```
SELECT * FROM products WHERE category = 'Gifts' OR 1=1--' AND released = 1
```

The new query will return all objects that fall into either the Gifts category or have a value of 1 in the category. The query will return all entries because 1=1 is always true.

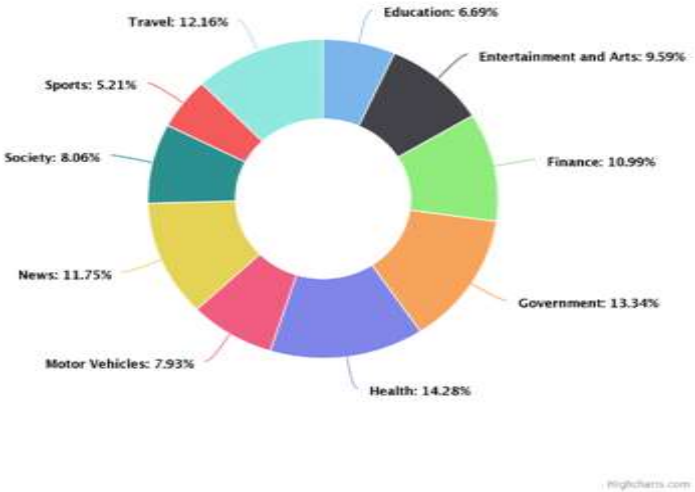

Figure 14: Distribution of SQL Injection in different Sectors
Source:Imperva

This Attack has a lot more areas to be discovered. The Author has mentioned only few of its characteristics Based on his Research and Developments. For more information, one can refer Internet.

Zero-Day Exploit Attack

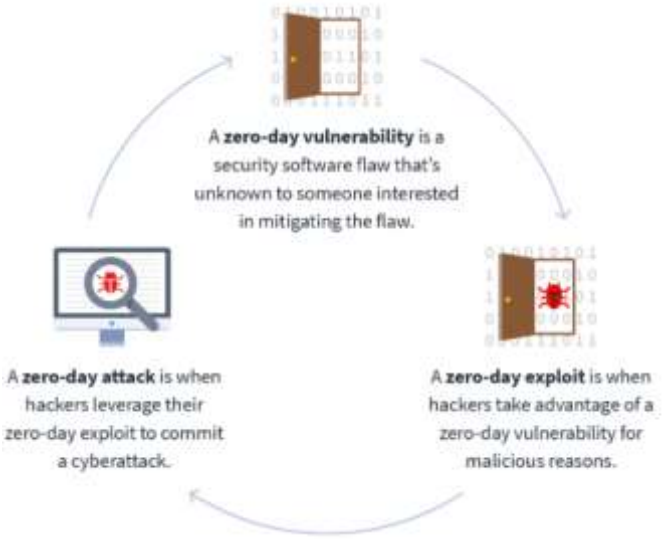

Figure 15: Basic working of Zero-Day Attack

At its root, a zero-day vulnerability is a defect, according to FIREEYE[10]. Software or hardware vulnerabilities can be exposed in the wild by an undiscovered exploit, which can cause a wide range of problems before anyone

notices. At first glance, a zero-day exploit is completely undetectable. It is referred to as a "zero-day attack" when an exploit is successfully carried out before the vulnerability has been fixed by the software's makers. For example, a zero-day attack occurs when attackers release malware before a developer has had an opportunity to repair the vulnerability—hence the term "zero-day," which describes a fault or software/hardware vulnerability that has been exploited. Let's have a look at the window of vulnerability step by step:

The developers of a company's software are unaware that their work contains a flaw. It's possible that a threat actor has already discovered or exploited this vulnerability before the developer has had an opportunity to do so. While the vulnerability is still open and available, the attacker writes and implements exploit code. In either case, either the public or the developer discovers the vulnerability and fixes it, preventing further damage to the system. An exploit is no longer a zero-day if a fix is created and used. These attacks are rarely discovered in the early stages of their development. In reality, it can take months or even years for a developer to discover the flaw that led to an attack, and it's not uncommon for this to happen.

Vulnerabilities introduced by zero-day patches can seem as any type of software flaw. Some examples include SQL injection, buffer overflows, faulty authorizations or URL redirection bugs, as well as issues with password security. This makes detecting zero-day vulnerabilities tough, which in some ways is a good thing because it also means that hackers will have a difficult time locating them. On the other hand, this also means that it is difficult to adequately protect against these vulnerabilities.

How to Protect Against Zero Day Attacks

Because zero-day attacks can take so many different forms, it's tough to stay safe from them. If a patch is not developed in time, almost any security flaw can be exploited as a zero-day. In addition, many software developers deliberately strive not to disclose the vulnerability in the hopes that they can deliver a fix before any hackers learn that the weakness is present.

In order to protect your company from zero-day attacks, you should implement the following strategies:

1. Stay informed
   It's rare to hear about a vulnerability that could be exploited in a zero-day attack, but it does happen. If you keep an eye on the news and your software providers' releases, you may be able to prevent an attack or respond to a threat before it is exploited.
2. Keep your systems updated
   In order to prevent exploitation, developers constantly try to keep their software updated and patched to the latest version. When a security flaw is found, a patch is released almost immediately. You and your team, on the other hand, are responsible for keeping your software platforms current at all times. Allowing automatic updates is the best course of action in this

situation because it ensures that your software is regularly updated without your involvement.

3. Employ additional security measures
   In order to protect yourself from a zero-day attack, make sure that you are employing security solutions that protect against this type of attack.

This Attack has a lot more areas to be discovered. The Author has mentioned only few of its characteristics Based on his Research And Developments. For more information, one can refer Internet.

Conclusion

When it comes to the survey's conclusion, it's evident that our generation has to be well-informed and vocal about cyber-attacks and risks, since we live in an easily exploitable environment. We cannot entirely prevent cyber-attacks, but our understanding of cyber-Norms and cyber-Ethics is the only alternative we have and on which we can rely. Strong cyber security policies should be developed in association with security awareness training and activities. Spam filters and anti-malware software can be installed. Installing endpoint detection and response (EDR) and deploying Next Generation Firewalls (NGFW) can help secure your systems. Organizations must have a staff of at least two or three information security engineers overseeing innovative software solutions and advanced cyber-attack testing in order to protect themselves from the most advanced threats. However, we should take basic security precautions such as using strong passwords, utilizing VPNs when accessing sensitive data, avoiding inserting/installing any unfamiliar device or application, and so on. These are some of the methods we may use to keep our data and privacy safe from attackers.

References

1. Statista:https://www.statista.com/statistics/249562/number-of-worldwide-internet-users-by-region/#:~:text=In%202021%2C%20East%20Asia%20accounted,Southern%20Asia%20with%20951.11%20million
2. https://www.statista.com/statistics/309435/india-cyber-crime-it-act/
3. Pintu Shah (SVKM's NMIMS Mukesh Patel School of Technology Management and Engineering, Mumbai, India): https://www.emerald.com/insight/content/doi/10.1108/ICS-04-2019-0041/full/html
4. Suman Acharya, Sujata Joshi: Impact of Cyber-Attacks On Banking Institutions In India: A Study Of Safety Mechanisms And Preventive Measures --Palarch's Journal Of Archaeology Of Egypt/Egyptology 17(6). ISSN 1567-214x
5. The HINDU: https://www.thehindu.com/business/cyberattacks-hit-26000-indian-sites-in-10-months/article37796297.ece
6. News 18: https://www.news18.com/news/india/83-organisations-in-india-reported-rise-in-phishing-attacks-during-covid-report-4224860.html
7. Delhi Cyber Cell : http://www.cybercelldelhi.in/cheatingscams.html

8. The Mint : https://www.livemint.com/news/india/83-organizations-in-india-saw-rise-in-phishing-attacks-during-pandemic-11632119876206.html
9. Sam Cook: https://www.comparitech.com/blog/informati on-security/ddos-statistics-facts/#:~:text=Research%20shows%20that%20the%20average,2021%20metric%20of%209.15%20Gbps.
10. Portswigger: https://portswigger.net/web-security/sql-injection
11. FIREEYES: https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html
12. purplesec: https://purplesec.us/prevent-cyber-attacks
13. A Sophos Article 04.12v1.dNA, eight trends changing network security by James Lyne.
14. Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole
15. Computer Security Practices in Non-Profit Organisations – A NetAction Report by Audrie Krause.
16. A Look back on Cyber Security 2012 by Luis corrons – Panda Labs.
17. International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 Page nos.68 – 71 ISSN 2229-5518, "Study of Cloud Computing in HealthCare Industry " by G.Nikhita Reddy, G.J.Ugander Reddy
18. IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2013.
19. CIO Asia, September 3rd , H1 2013: Cyber security in Malaysia by Avanthi Kumar.
20. https://encyclopedia.kaspersky.com/knowledge/vulner abilities-examples/
21. Hardware Security, Vulnerabilities, and Attacks: A Comprehensive Taxonomy, Paolo Prinetto and Gianluca Roascio, CEUR-WS.org/Vol-2597/paper16.pdf
22. 2https://economictimes.indiatimes.com/definition/denial-of-service-attack
23. https://www.cloudflare.com/en-in/learning/ddos/whatis-a-ddos-attack/
24. Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. Procedia Economics and Finance, 24-31. doi:10.1016/S2212-5671(15)01077-
25. Cabaj, K., Kotulski, Z., Księżopolski, B., & Mazurczak, W. (2018). Cybersecurity: trends, issues, and challenges. EURASIP Journal on Information Security. doi:10.1186/s13635- 018-0080-0 127 Unauthentifiziert | Heruntergeladen 01.09.19 21:18 UTC HOLISTICA Vol 10, Issue 2, 2019
26. Dervojeda, K., Verzijl, D., Nagtegaal, Lengton, M., & Rouwmaat, E. (2014). Innovative Business Models: Supply chain finance. Netherlands: Business Innovation Observatory; European Union.
27. Gade, N. R., & Reddy, U. G. (2014). A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies. Retrieved from https://www.researchgate.net/publication/260126665_A_Study_Of_Cyber_Security_Ch allenges_And_Its_Emerging_Trends_On_Latest_Technologies
28. Gross, M. L., Canetti, D., & Vashdi, D. R. (2017). Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. Journal of Cybersecurity, 3(1), 49–58. doi:10.1093/cybsec/tyw018
29. Hua, J., & Bapna, S. (2013). The economic impact of cyber terrorism. The Journal of Strategic Information Systems, 22(2), pp. 175-186.

30. Kumar, S., & Somani, V. (2018). Social Media Security Risks, Cyber Threats And Risks Prevention And Mitigation Techniques. International Journal of Advance Research in Computer Science and Management, 4(4), pp. 125-129.
31. Panchanatham, D. N. (2015). A case study on Cyber Security in E-Governance. International Research Journal of Engineering and Technology.
32. Samuel, K. O., & Osman, W. R. (2014). Cyber Terrorism Attack of The Contemporary Information Technology Age: Issues, Consequences and Panacea. International Journal of Computer Science and Mobile Computing, 3(5), pp. 1082-1090.
33. Sharma, R. (2012). Study of Latest Emerging Trends on Cyber Security and its challenges to Society. International Journal of Scientific & Engineering Research, 3(6).
34. Sreenu, M., & Krishna, D. V. (2017). A General Study on Cyber-Attacks on Social Networks. IOSR Journal of Computer Engineering (IOSR-JCE), 19(5), pp. 01-04. [12] Sutton, D. (2017).
35. Cyber Security : A Practitioner's Guide. Swindon, UK: BCS, the Chartered Institute for IT
36. [1]. Daniel, Schatz,; Julie, Wall, (2017). "Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law. 12
37. ISSN 1558-7215. Archived from the original on 28 December 2017. [2]. Rouse, Margaret. "Social engineering definition". Tech Target. Archived from the original on 5 January 2018. Retrieved 6 September 2015.
38. Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017). "Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law. 12 (2). ISSN 1558-7215.
39. "Reliance spells end of road for ICT amateurs", 7 May 2013, The Australian
40. Stevens, Tim. "Global Cyber security: New Directions in Theory and Methods". Politics and Governance. 6 (2). doi:10.17645 /pag.v6i2.1569.
41. "Computer Security and Mobile Security Challenges". researchgate.net. Archived from the original on 12 October 2016. Retrieved 4 August 2016.
42. "Distributed Denial of Service Attack". csa.gov.sg. Archived from the original on 6 August 2016. Retrieved 12 November 2014.
43. Wireless mouse leave billions at risk of computer hack: cyber security firm Archived 3 April 2016 at the Way back Machine.
44. "Multi-Vector Attacks Demand Multi-Vector Protection". MSSP Alert. July 24, 2018.
45. Millman, Renee (December 15, 2017). "New polymorphic malware evades three quarters of AV scanners". SC Magazine UK.
46. Turner, Rik (May 22, 2018). "Thinking about cyber-attacks in generations can help focus enterprise security plans". Informa PLC. Ovum.
47. "Identifying Phishing Attempts". Case. Archived from the original on 13 September 2015.
48. Arcos Sergio. "Social Engineering" (PDF). Archived (PDF) from the original on 3 December 2013.
49. Scannell, Kara (24 February 2016). "CEO email scam costs companies $2bn". Financial Times (25 Feb 2016). Archived from the original on 23 June 2016. Retrieved 7 May 2016.

50. "Bucks leak tax info of players, employees as result of email scam". Associated Press. 20 May 2016. Archived from the original on 20 May 2016. Retrieved 20 May 2016