An Overview on Cyber Attacks : Impacts and Mitigations

Hashida Haidros
Central University of Kerala
7 PUBLICATIONS **51** CITATIONS
SEE PROFILE

Manohar Naik S
Central University of Kerala
23 PUBLICATIONS **116** CITATIONS
SEE PROFILE

Data Mining & Predictive Analytics (2021): 69-84
Editors: V. Kumar, R.Rajesh, T.M Thasleema & S. Manohar Naik
Central University of Kerala, Kasargod
Today & Tomorrow’s Printers and Publishers, New Delhi – 110002
ISBN 10:81-7019-700-6 ISBN 13: 9878170197993

An Overview on Cyber Attacks : Impacts and Mitigations

Hashida Haidros Rahima Manzil , Dr. Manohar Naik S

Abstract

As the modern society depends on technological infrastructure more than ever before,the digital data creation has surged and vulnerable to cyber-attacks. The need to expedite cyber security adoption is paramount. Since the attackers have emerged with innovative techniques and tools, the implementation of effective cyber security measures becomes challenging and crucial today. According to studies in the year 2018, India was ranked second position(17%) to be affected by cyber crimes and the US holds top position (38%) .Spending on Cyber security will reach $6 trillion by 2021. The authorized cyber professionals claiming that technology has to competitive with advanced techniques followed by attackers because impacts and loss of cyber attacks in various fields challenging the need of advanced cyber security. In this paper an overview of Cyber attacks,impacts and statistics are discussed and necessary mitigation approaches are also provided.

Keywords – c*yber-attacks, cyber security, cyber crimes*

I. INTRODUCTION

In past few years the internet usage has rapidly increased due to emergence of internet based facilities. These facilities has captured the human race in a world of internet technologies and encouraged the massive use of internet. This has resulted in the huge data transfer and information generation. With the times attackers have also become intelligent and developed advanced devices and ways to attack the network and steal the information in an anonymous way. [19]Cyber Security is a practice of protecting sensitive data or information as well as other communication systems from, unauthorized access, interception or exploitation or even from theft. [19]The government, national defence system, banks, hospitals, corporate, research and development organization etc., may hold highly confidential data and even small amount of negligence to these data may cause an extensive amount of loss. Even the security and privacy of data belongs to an individual is vital. Therefore, security in cyber space is inevitable.

For any business, a data breach can cause huge consequences. It can unravel a company’s reputation through the loss of consumer and partner trust. The loss of critical data, such as sensitive files or compromising intellectual property, can cost a company to a demolition. Going further, a data breach can impact corporate revenues because of non-compliance with data protection regulations. It’s estimated that, [22]on average, a data breach costs an affected organization $3.6 million. It’s essential for organizations to adopt and implement a strong cyber security approach in order to keep up with security standards as well as to take necessary safeguard against illegal activities. Another dangerous fact is that those criminals, terrorists, and spies rely heavily on cyber-based technologies ,the national or international defence systems are now under utmost cautious. This is the reason that everyone encouraged to gaze Cyber security and its adversary measures.

The paper is organized as follows, Section I contains the Introduction of the Cyber security, Section II contains the discussion of different types of Cyber Attacks, Section III contains the discussion of major impacts of Cyber attacks, Section IV contains the discussion of some of the Mitigation approaches, and Section V concludes the paper.

II. COMMON CYBER THREATS

Malware attack [28]Malicious software that is installed in systems without the knowledge of user can be refered as malwares. [28]It attached to legitimate code and propagate through internet. It will be hidden in useful applications or replicate itself across the Internet. Following describes some common types of malwares :

Macro viruses — These viruses written in macro language. [28]The applications such as Microsoft Word or Excel are the common platforms for macro viruses, in which the macro facility used to execure routine tasks frequently cause the malicious code to be activate. When the application once opened, the virus get executed, consequently sequence of malicious actions should begin to run automatically before transferring control to the application. It is self-replicative and can attach to other legitimate code in the computer system.

File infectors — [28]A kind of viruses that usually attach themselves to executable code, such as .com, .exe files. The virus code will get executed while the file get opened. The operating systems including Windows, UNIX and Macintosh are the major victims of this file infectors.

System or boot-record infectors — [28]This kind of virus infects the executable code found in boot sector of floppy disks or it attached to the master boot sector on hard disk. Then the system begins to boot from an infected disk, it will load the virus into memory, where it can propagate to other disks and computers. This type of viruses has become very rare now.

Polymorphic viruses — [28]These viruses can change themselves while keeping its original algorithm intact through varying cycles of encryption and decryption. In order to vary its physical signature during each infection, polymorphic viruses encrypts code everytime and also changes the keys as well. Everytime it infects a machine, it relys on mutation engines to change decryption routine continuously. Thus makes difficult to detect due to continuous change of their signature.

Stealth viruses — [28]Stealth viruses are hidden viruses in which harmful code functions will be hidden in computer memory and also its self replicas will resides in undetectable areas of system, thus tricking anti-virus softwares by keeping itself undetectable, sometimes make anti-virus softwares to inform that the actual infected areas are un-infected. The first known virus for PC, Brain was a Stealth virus.

Trojans — [28]A Trojan or a Trojan horse is a program that looks harmless, acts as legitimate but inside contains some malicious function. Trojans do not self-replicate. Trojan establishes a back door that can be exploited by attackers. Usually when the victims clicks on some innocent looking emails or free downloads, the malicious code has begin to execute and the victims doesn’t suspect that the attachment is actually a Trojan horse.

Logic bombs — [28]A type of malicious software that is embedded into a program or appended to an application. The logic bombs get triggered based on some logical critera or whenever a specific event has occured, for example when a logical condition achieved or a specific date and time being reached.

Worms — [28]Instead of attached to a host file, worms are self-contained, stand alone programs that spread across networks and computers by exploiting operating systems vulnerabilities. Worms are commonly spread through email attachments and opening the attachment will cause the worm to activate. A worm propagating across the internet may cause overloading email servers, which further results denial-of-service attacks against nodes on the network.

Droppers — [28]A dropper is a program designed to install or drops, malwares/viruses on targeted systems. The dropper is like a trojan which is not infected itself with malicious code but drops viruses on targeted system when it gets run and, therefore might not be detected by virus-scanning software. A dropper once activated, can download updates to virus software as well.

Ransomware — [28]Ransomware is a type of malware that encrypts the victim's data and thereby blocks access to those data and threatens to delete it unless a ransom is paid. The attacker will provide a message, asks victims for ransome money as bitcoins and also provide a sample decrypted data to victims. Within some time limit the victims prompted to pay the ransome otherwise data may loss . The ransomeware may cause a huge business loss , even that small time delay can cost tremendous loss for business.

Adware — [28]Adware is a kind of malware, which is extensively promoted by companies as part of their marketing purposes. The pop-up advertising banners get appeared while any program is executing. It can be automatically downloaded to the system while browsing any in secured website and can be viewed through pop-up windows or through a bar that appears on the computer screen automatically.

Spyware — [28]Spyware is a type of program as its name indicates, it works as spy agent in order to collect information about users, their computers or their browsing habits. It tracks everything without user's knowledge and sends the data to the corresponding system of attacker. Usually the systems get infects through downloading materials from unknown sources or accepting pop-up advertisements or opening email attachments from unrecognized sender etc. Spywares are able to redirect web searches and reset the web homepage as well.

Phishing and Spear Phishing **[21]**Phishing attack is the practice of obtaining sensitive information like credit card details, or login credentials by masquerading as legitimate entity in an electronic communication. It can be treated as social engineering attack. Phishing email typically consists of link to websites that are infected with malicious code, there by trick user into downloading malware or handing over personal information. [28]In the case of Spear phishing attackers take the time to conduct research to analys targets and create legitimate messages that are personal and relevant. Email spoofing is one of an example of spear phishing. Another technique which is common among hackers is, website cloning in which hackers create a replica of some legitimated websites and thus make users fool themselves by imitating as the genuine one , hence tricking them to enter personally identifiable information (PII) or login credentials.

Cryptojacking **[17]**It is a form of cyber attack in which a hacker hijacks a target's processing power to mine crypto-currency on the hacker's behalf. Cryptojacking make use of malware via a script loaded into a web browser to steal unused CPU cycles and use them to perform cryptomining calculations. Cryptojacking can be done by directly infecting a device with malware, or by indirectly stealing processing cycles of cpu whenever user visits a less secured and compromised website. Another variation in Cryptojacking may consists injecting malicious JavaScript into a vulnerable website. The victims once browse such an infected site will have their CPU cycles hijacked to perform cryptomining.

- [17]In 2018, around 25% of businesses have been the victims of Cryptojacking.
- [17]In February 2018, a Spanish cybersecurity firm, Panda, wrote that a cyrptojacking script known as WannaMine, a malware was being used to mine monero, a cryptocurrency that is notable for its ability to mine using CPUs
- [17]According to a recent Fortinent report, Cryptojacking malware grew from impacting 13% of all organizations in Q4 of 2017 to 28% of companies in Q1 of 2018, more than doubling its footprint.
- [17]Later in February,Tesla Inc. had get cryptojacked.

Drive-by-attack **[25]** With this type of attack, Hackers rely on browser exploit packs(BEP), the automated exploit framework, consists of bundle of exploits which is used to initiate malware. The attackers plant a malicious script into HTTP or PHP code on any one of web pages. This script might install malware directly onto the targeted system of someone who visits the site, or it might re-direct the victim to a site controlled by the hackers. Drive-by downloads The drive-by attack doesn’t rely on a user to click a button or open a malicious email attachment, merely visiting some malicious untrusted website , may cause download the malware.

SQL-injection attacks SQL injection has become one of a serious vulnerability in database-driven websites. It occurs when an attacker embedd malicious code with strings which is then passed to the database for execution. Thus the query results can capture sensitive data such as credit card details or usernames or passwords. [23]Improper user input validation, server-side variable modification, cookie tampering etc., are considered as major reasons behind SQL injection attacks.

Cross-site scripting (XSS) attack [28]It occurs when the client visit the web page that runs malicious code. It is a client side code injection attack in which the attacker injects a payload with malicious JavaScript into a website’s database. When the victim requests a page from the website, the corresponding page with the attacker’s payload as part of the HTML body will be transmitted to the victim’s browser, which executes the malicious script. [16]Once the malicious code get executed successfully, the attacker might then be able to access browser cookies. This also enables an attacker to log key strokes, capture screen shots and acquire sensitive network information, and remotely monitor the victim’s machine.

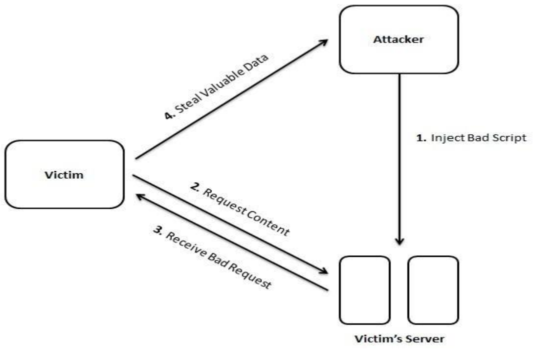

Fig1. Diagram of Cross-site scripting attack

Eavesdropping attack The interception of network traffic may cause eavesdropping attacks. [28]It is the practice of obtaining usernames or passwords, credit card numbers and other confidential information that a user might be transmitting over the network. Two types of eavesdropping are there, passive or active:

Passive eavesdropping — [28]A hacker detects the information without any scanning , just by listening to the message transmission in the network.

Active eavesdropping — [28]A hacker grabs the information by actively disguising himself as friendly unit and by sending queries to transmitters. This is called probing, scanning or tampering.

Birthday attack **[27]**Birthday attacks relys on Birthday problem, which aims to find the probability of two birth dates to be the same. This birthday paradox can be applied against hash algorithms that are used to ensure the integrity of a message, or digital signature. A message processed by a hash function produces a message digest (MD) of fixed length, independent of the length of the input message; this MD uniquely characterizes the message. [28]The birthday attack designed to produce two random messages that generates the same MD when processed by a hash function, then the attacker enables to rewrite user’s message and the receiver will not be able to detect the correption.

DoS attacks DoS (denial-of-service) attacks refers to the disruption of normal web traffic of a targeted network or service of some server by flooding systems, servers or networks with more requests beyond the level that they can handle, causing them to crash.

DDoS (distributed denial of service) is a type of DoS attack in which many distributed sources involves. [27]DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. The machines including computers, network devices or other IoT devices can get exploited . When multiple systems together orchestrate a synchronized DoS attack to a single target, it known as DDoS attack. In this case the target is attacked from many locations at once rather than from a single point of location.

A few common DoS attacks include:

Smurf attack – A common type of distributed denial-of-service (DDoS) attack in which an attacker attempts to flood a targeted server with Internet Control Message Protocol (ICMP) packets. By making requests with the spoofed IP address of the targeted device to one or more computer networks, thus causes the initial attack traffic and potentially overwhelming the target network making it inaccessible.

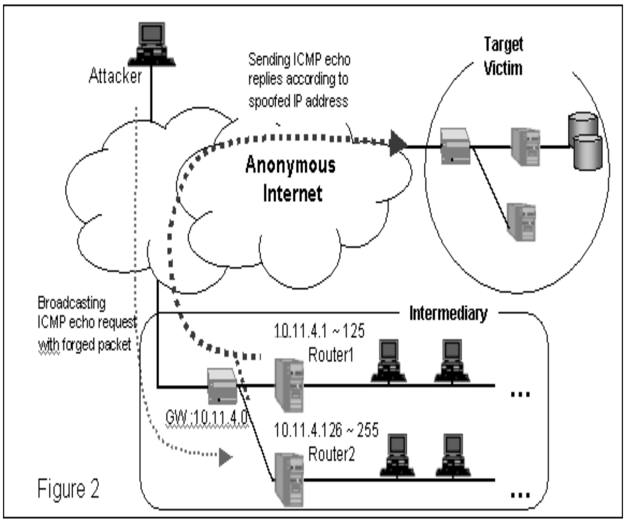

Fig2. Diagram of Smurf Attack

Ping flood – A kind of simple denial-of-service attack which aims to overwhelm a target server with ICMP ping packets. By flooding a target with a number of pings than it is able to respond to efficiently, causes denial-of-service .

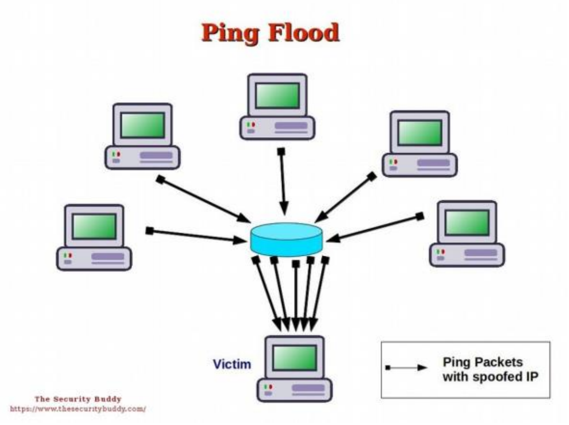
Ping Flood
Victim
Ping Packets with spoofed IP
The Security Buddy
https://www.thesecuritybuddy.com/

Fig3. Diagram of Ping Flood Attack

Ping of Death - [28] It is a kind of denial-of-service (DoS) attack, in which the attacker disrupts a targeted machine by sending a packet larger in size, exceeds its maximum allowable size limit then causing the target machine to get crashed. This kind of attack uses IP packets to ping a target system with an IP size which exceeds maximum limit of 65,535 bytes. IP packets of this size are not allowed, so attacker fragments the IP packet. When the target system reassembles the packet, it may generate buffer overflows and other crashes.

Buffer overflow attacks – [29]A buffer is a temporary area for data storage. When the data to be stored exceeds its allocated size, the extra data get overflows. It then causes some of that data to leak out into other next buffer, which can corrupt or overwrite its original data they were holding. In a buffer-overflow attack, the extra data sometimes holds specific malicious instructions for actions intended by a hacker, for example, the data could trigger a response that corrupt files, modifies data or unveils private information. Attacker can make use of this buffer-overflow exploit to take advantage of a program that is waiting on a user's input. Facebook on November 14th 2019 posted a security advisory about a seriously risky buffer overflow vulnerability in WhatsApp, **CVE-2019-11931**, that could be triggered by a nastily crafted MP4 video. It indicates a potential risk vulnerability, whenever it left un-patched, it may lead to further malicious processes like remote code execution, which enables attackers to access users' files and messages. The security hole also leaves devices vulnerable to Denial of Service (DoS) attack.

ICMP flood – This attack leverages mis-configured network devices with the help of spoofed packets that ping every computer on the targeted network. The network is then triggered to initiate the traffic.

TCP SYN flood – [28]In this attack, during a Transmission Control Protocol(TCP) session initialization handshake, an attacker exploits the buffer space. The attacker aims to floods the target system's process queue with connection requests, and unnecessarily delays the response with target system's requests. Consequently a time out will occur while waiting for the response from the attacker's device, thus makes the system to crash or become unusable when the connection queue fills up.

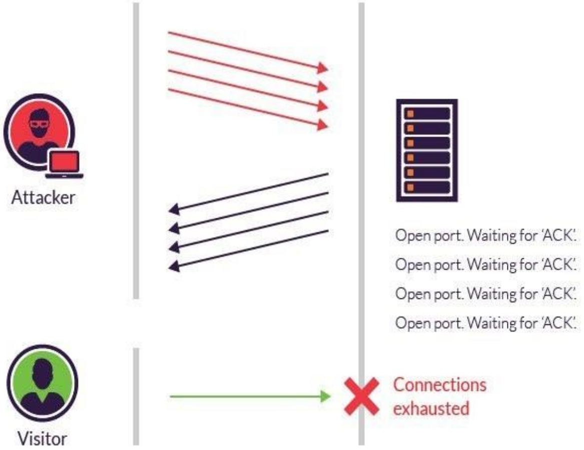
Attacker
Open port. Waiting for 'ACK'.
Open port. Waiting for 'ACK'.
Open port. Waiting for 'ACK'.
Open port. Waiting for 'ACK'.
Visitor
Connections exhausted

Fig4. Diagram of TCP SYN flood

***Teardrop attack* -** [30]A kind of denial-of-service (DoS) attack in which fragmented packets will be sent to a target machine. Since the machine receiving such packets cannot reassemble them , the packets get overlapped with one another, crashing the target network device. This attack is very rare today, generally effects older operating systems. [28]In order to protect from this attack, disable SMBv2 and block ports 139 and 445.

***Botnets* - [31]**Botnets are the millions of compromised systems infected with malware under hacker control in order to carry out DDoS attacks. [31]Two advanced botnet mechanisms includes Fast flux and Domain flux. In Fast flux mechanism, a set of IP addresses change frequently corresponding to unique domain name. The later mechansim designed to generate set of domain names automatically corresponding to unique IP address.

Man-in-the-Middle attack (MitM) This type of attack occurs when an attacker positions himself between the communications of a client and a server. Some common types of man-in-the-middle attacks includes:

***Session hijacking* -** [32]In this attack, an attacker exploits valid computer session and aquires session Identifier of victim thus masquerading as authorized user. The IP address will be replaced as of the trusted client, thus making the server believe that it is communicating with the actual client.

***IP Spoofing* –** [28In this attack, the attacker masquerades as trustworthy enity, thus enables to access the system. The attacker transmits a packet with the IP source address of a known, trusted host to a target host. The target host might accept the packet believing that arrives from legitimate source and proceeds further.

***Replay* -** [28]A replay attack occurs when an attacker aims to intercepts the network and fraudulently retransmit or delayed data transmission.The Session timestamps can be used as counter measures for this type of attack.

Backdoors [22]As per Palo Alto Networks, The Iran-linked Chafer threat group has used a new Python-based backdoor in November 2018 attacks targeting a Turkish government entity. Backdoors refers to any procedure by which authorized and unauthorized users are able to get around normal security measures and gain root access on a computer system, network, or software application. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting to resolve software issues. But the attackers often use backdoors for negative intention as part of an exploit.

III. IMPACTS OF CYBER ATTACKS

It's been evident that cyber attacks can have numerous negative impacts. [11]According to the researchers from the University of Oxford and Kent's School of Computing, the impact of cyber attacks can be classified based on five key themes including, physical or digital, economic, psychological, reputational and social or societal. Each category undelines the significant impacts of cyber attacks. The physical/digital category lists the loss/damage of infrastructure. The economis category lists reduced profits and all financial loss. The psychological category lists personal depression, embarrasement and feel of confused etc.,The reputational impacts may include loss of key staffs, damaged customer relationships. In societal/social level the impacts can be viewed as a risk of disruption from daily life, a negative perception of technology or lack of internal morale in organizations. The following statistics[17]on various attacks, including malware, ransomware ,social engineering and phishing, is described to give an overview of cyber attack impacts.

1. Malware Statistics

Malware or malicious software is any software intentionally designed to cause damage to a computer, server, client, or computer network. A wide variety of types of malware exist, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, and scareware. Malware attacks can occur on all sorts of devices and operating systems, including Microsoft Windows, macOS, Android, and iOS. Malware seem to get more sophisticated every year. Because it is often difficult to detect, and devices are typically infected without the user even noticing, it can be one of the primary threats to your personal information and identity that you must be on guard for. Malware has infected roughly a third of the world's computers, costing companies across the globe trillions of dollars each year. In 2014, nearly 1 million new pieces of malware were released every day[17], but most hackers relied on old techniques to create new threats. Today, threats are increasingly sophisticated, and as web traffic volume grows and more connected devices come online, the attack surface is rapidly expanding.

Table1: The total malware infections for the last 10 years [17]:-

YEAR	Tot.infections(%)
2009	12.4
2010	29.97
2011	48.17
2012	82.62
2013	165.81
2014	308.96
2015	452.93
2016	580.40
2017	702.06
2018	812.67

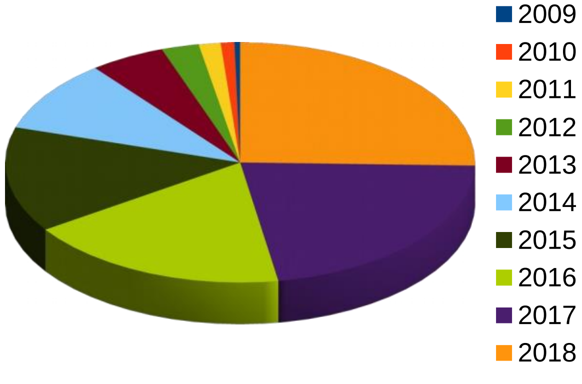

Fig.5 piechart of total malware infections for last 10 years[17]

2. Ransomware Statistics

In 2018 Ransomware attacks world wide rose 350%. [17]It has been estimated to cost around $6 trillion annually by 2021, it costs businesses more than $75 billion per year. The popular ransomware attack, Notpeyta has cause loses that exceeds $1 billion. The company named FedEx, one of a victim of Notpeyta ransomware attack, lost an estimated $300 million in 2017. In march 2018, the companies including atlanta , georgia has spent more than $5 million for rebuilding their computer network, after being attacked from the Sam Sam ransomware. In 2019 ransomware from phishing emails increased 109% over 2017. [17]According to studies in 2019, in every 14 seconds a new organization will become victim to ransomware, and every 11 seconds by 2021. According to the Kasperasky statistics(fig6.) number of new ransomware modifications fell markedly against Q4 2018 tothe level of Q3. Seven new families were identified in the collection.

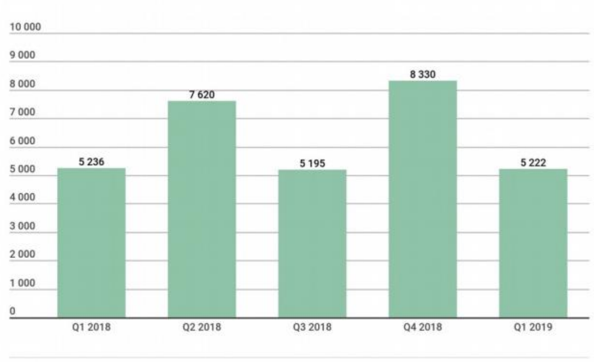

Fig.6 Chart of Ransomware statistics as per kasperasky[15]

3. Social Engineering Statistics

The way used in social engineering type attacks is the psychological manipulation of people into performing actions or revealing confidential information. [17]It is evident that 98% of cyber attacks rely on Social engineering, it hit more than 500% from the first to second quarter of the year 2018. The famous American computer security consultant, *Kevin Mitnick* said in his article that "*You could spend a fortune purchasing technology and services...and your network infrastructure could still remain vulnerable to old-fashioned manipulation.*" The one thing that everyone seems to agree upon is that social engineering is generally a hacker's clever manipulation of the natural human tendency to trust. The hacker's goal is to obtain information that will allow him/her to gain unauthorized access to a valued system and the information that resides on that system. The following table (Table2)describes percentage of breach incidents on the basis of its types. Associated chart is given in figure.7.

Type of breach	**Number of attacks (%)**
Identity theft	65%
Account access	17%
Financial access	17%
Nuisance	4%
Existential data	1%

Table2:percentage of breach incidents on the basis of its types.[17]

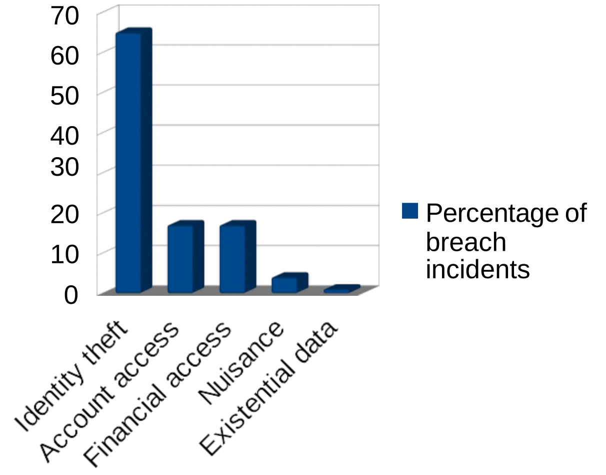

Fig7[17] Chart of breach incidents on the basis of type

4. Phishing Statistics

Phishing is a type of cyber attack where threat actors randomly send emails to a broad audience in an attempt to trick people into providing sensitive information such as account credentials or sensitive information. [17]In 2018, 83% of global infosec respondents experienced phishing attacks, an increase from 76% in 2017. [17]Also in 2017, the Business Email Compromise (BEC) scams cost organizations $676 million. [17]The surveys revealed that approximately 30% of phishing messages get opened by targeted users and 12% of those users click on the malicious attachments or link. [17] The studies in 2017 revealed that around 53% of IT and security professionals admits they have experienced a phishing attack. [17]Also 50% of phishing sites are now using HTTPS. [17]The volume of email fraud that organizations faced has increasing 8% in every year. The following table(Table3) describes most common malicious attachment types and its percentage of occurrences in the year 2018, and Fig8. is the related chart.

Malicious Attachment types	**Number of incidents(%)**
Office	38%
Archive	37%
PDF	14%
Other Ext	6%
Binaries	4%
XML/HTML/JS	1%

Table3: Number of phishing incidents(%) on different attachment type[17]

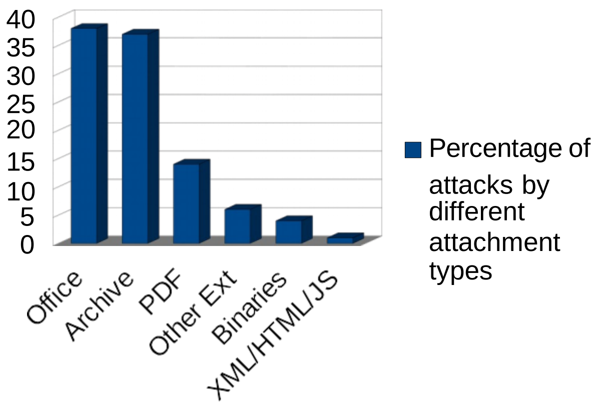

Fig.8 Chart of Number incidents on different attachement types[17]

III. MITIGATIONS

According to ASD[7] (Australian Signals Directorates), the Australian government agency responsible for foreign signals intelligence, a list of strategies provided in order to mitigate cyber security incidents. A single mitigation approach is not enough to prevent cyber security incidents. In order to develop strategies to help reduce malware, the preferred method should include a layered approach using proactive and reactive mechanisms throughout the network. Indeed Anti-virus software plays a key role in this area; however, it alone may not help in some times. Also an old version of anti-virus may cause more vulnerabilities in system. Some of the essential mitigation approaches to prevent malware delivery and execution are discussed below :

Application whitelisting : [7]It prevents installation or use of unauthorised applications. It ensures that only authorised applications can be executed on systems.

Patch applications : [7]A 'patch' refers to some changes to a computer program which designed to fix vulnerabilities . The system security can be ensured by applying patches properly in a timely manner. [7]The recommended time frames for applying and verifying patches are described below:

1. extreme risk: indicates the deadline within 48 hours after a patch being released
2. high risk: indicates the deadline within two weeks after a patch being released
3. moderate or low risk: indicates the deadline within one month after a patch being released

Configure Microsoft Office macro settings : [7]In Microsoft Office applications macros can be used to execute frequently used tasks. However, macros can contain malicious code. Therefore to manage macros, only allows trusted macros to be used in applications which should be digitally signed with authorized certification.

User application hardening : [7]It refers to configuring web browsers in order to block Flash, advertisements and other untrusted code on the Internet. It should disable unnecessary features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.

Email content filtering : [7]Email content filtering helps to prevent the compromise of user computers via adversaries using malicious emails. Whitelisting business-related attachment types is significantly more effective than attempting to identify and blacklist a complete list of malicious file types and file extensions, including those increasingly leveraged by adversaries such as .lnk shortcut files, PowerShell and JScript files.

Mitigation strategies taken to limit the extent of cyber security incidents :

Restrict administrative privileges : [7]In organizations various kinds of users may exists each having different privileges. Those users with administrative privileges are able to make significant changes to operating system configurations and application data bases. In order to prevent any malicious internal activity, organizations have recommended to control administrative privileges. Thus by restricting administrative privileges may reduces the potential damage of any malwares or prevents from those attacks.

Multi-factor authentication : [7]In order to prevent unauthorized access to any device or network, multi-factor authentication supports double security to sensitive information. Multi-factor authentication involves users verifying their identity by using at least any two of the three mechanisms: something the user knows, such as a passphrase or PIN, something the user has, such as a physical token or software-based certificate and something the user is, such as their fingerprint or iris.

Mitigation strategy taken to recover data and system availability :

Daily backups : [7]It is highly recommended to keep up daily backups of everything which stored, transmitted over cyber space. To ensure the availability of information even after any cyber attack incident has occurred, there should be daily backups of important new/changed data, software and configuration variables.

IV. CONCLUSION

As we look towards this decade of digital world which has been driven by rapidly evolving Technology, It's clear that Cyber security has a remarkable role in everyone's daily life with the dependence to the Technological advancement is increased through social networking, online transactions, business organizations and other automation processes etc. While with the technogocical advancement, the attackers continuosly developing new threats and tools to breach over security measures of industries and government organizations. The study states that approximately three out of every ten Indian cyber users encountered one or more cyberattacks. So it is important to aware of various cyber attack types. In this paper we have discussed different attack types and its impacts in various level. And we have also discussed some mitigation approaches.

REFERENCES

[1] David Salomon, Foundations of Computer Security, Springer, 2006.

[2] William Stallings, Network Security Essentials: Applications and Standards, Prentice Hall, 4th edition, 2010.

[3] 'From information security to cyber security'. Rossouw von Solms, Johan Van Niekerk. https://doi.org/10.1016/j.cose.2013.04.004

[4] 'Leveraging cyber threat intelligence for a dynamic risk framework'. R.Riesco, V.A Villagra. International Journal of Information Security (2019)

[5] Malware Analysis. In Proceeding of the IEEESymposium on Security and Privacy, Oakland, California, USA, pages 231.

[6] 'DdoS attack detection with feature engineering and machine learning : the framework and performance evaluation'. Muhammad Aamir and Syed Mustafa Ali Zaidi. International Journal of Information Security 18, 761-785(2019)

[7] 'Srategies to Mitigate Cyber Security Incidents-Mitigation Details'.ASD (Australian Signals Directorate)

[8] A Survey on Cyber Security Threats and Challenges in Modern Society. Sayeed Z.Sajal;Israt Jahan, Minot, ND, USA. 2019 IEEE International Conference on Electro Information Technology (EIT)

[9] Indian Computer Emergency Response Team (CERT-In). Annual Report 2018, 2017

[10] 'An Investigation on Cyber Security Threats and Security Models'. Kutub Thakur, Meikang Qiu, Keke Gai, Md Liakat Ali. 2015 IEEE 2 nd International Conference on Cyber Security&Cloud Computing.

[11] 'A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate'. Ioannis Agrafiotis, Jason R C Nurse, Michael Goldsmith, Sadie Creese, David Upton *Journal of Cybersecurity*, Volume 4, Issue 1, 2018, tyy006, https://doi.org/10.1093/cybsec/tyy006

[12] Malware Analysis and Mitigation in Information Preservation. Aru Okereke Eze and Chiaghana Chukwunonso E. Department Of Computer Engineering, Michael Okpara University Of Agriculture, Umudike Umuahia, Abia State-Nigeria.

[13] 'The rise of crypto–ransomware in a changing cybercrime landscape:Taxonomising countermeasures' . Lena Y.connolly, David S. Wall. https://doi.org/10.1016/j.cose.2019.101568

[14] The Evolution to Fileless Malware. David Patten. East California University

[15] Kasperasky : https://www.kasperasky.co.in

[16] 'Prevention of Cross-site Scripting Attacks on Current Web Applications'. Joaquin Garcia Alfaro, Guillermo Navarro-Arribas. OTM Confederated International Conferences "On the Move to Meaningful Internet Systems"

[17] Purple Sec Blog : https://purplesec.us

[18] SentinelOne Blog: https://www.sentinelone.com

[19] https://www.tutorialspoint.com

[20] Cisco security. https://www.cisco.com

[21] 'A Study of Preventing Email (Spear) Phishing by Enabling Human Intelligence'. Nathalie Stembert ; Arne Padmos ; Mortaza S. Bargh ; Sunil Choenni ; Frans Jansen . IEEE 2015 European Intelligence and Security Informatics Conference.

[22] Security Week : www.securityweek.com

[23] 'Securing web applications from injection and logic vulnerabilities: Approaches and challenges'. G.Deepa, P.Santhi Thilagam. Information and Software Technology.https://www.elsevier.com

[24] https://www.cyberswachhtakendra.gov.in

[25] 'Drive- By Download Attacks: A Comparative Study'. Aditya K.Sood, Sherali Zeadally. IEEE

[26] Forcepoint Blog : https://www.forcepoint.com

[27]“Another birthday attack”, D. Coppersmith, *Advances in Cryptology, Proc. of Crypto’85*, LNCS, vol. 218, Springer-Verlag, 1986, pp. 14–17.

[28] https://blog.netwrix.com

[29] https://geeksforgeeks.com

[30] https://radware.com

[31] ‘A Survey on latest Botnet attack and Defense’.Lei Zhang, Shui Yu, Di Wu, Paul Watters. 2011 International Joint Conference of IEEE TrustComm-11/IEEE ICESS-11/FCST-11

[32] ‘Session hijacking attacks in wireless networks: A review of existing mitigation techniques’. Enos Letsoalo, Sunday Ojo. IEEE