ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 11 Issue 6 June 2024

Cyber Security: Types of Attacks

[1] Shravani Kulkarni, [2] Dhawal Kumbhare, [3] Arya More, [4] Radhika Purandare

[1] [2] [3] [4] Vishwakarma Institute of Information Technology (VIIT), Pune India

Corresponding Author Email: [1] shravani.22111224@viit.ac.in, [2] dhawal.22110913@viit.ac.in, [3] arya.22111232@viit.ac.in, [4] radhika.purandare@viit.ac.in

Abstract*— In today's digital environment, where many attacks threaten important information and important processes, cyber security is still the most important topic, especially in computer networks. This article provides an in-depth look at the various types of attacks available on computer networks and explores the evolving strategies cybercriminals use to exploit vulnerabilities and infiltrate systems. The research draws on professional, international legal, and international research data to provide a comprehensive analysis of cyber threats and countermeasures seen worldwide in the past year. It identifies malware, phishing, DDoS (distributed denial of service), ransomware, and insider threats, showing their mechanisms and potential impacts on organizations and individuals. Additionally, this article explores emerging cyberattacks in the Internet of Things (IoT) ecosystem and digital substations, including business plans, and highlights security challenges specifically designed by Industry 4.0 standards and distributed hardware and software architectures. By combining research results and recommendations, this article provides recommendations for improving cyber defense strategies, including threat detection, strong authentication mechanisms, encryption protocols, and personnel training. This research aims to promote a deeper understanding of cyber threats and vulnerabilities in computer networks, helping stakeholders develop strategies to mitigate and prevent change.[1].

***Index Terms*— Vulnerabilities, Countermeasures, Cyber threats, Computer Networks.**

I. INTRODUCTION

In today's interconnected digital environment, cyber threats pose serious challenges to protecting important information and critical systems, especially in computer networks. Cyber Security remains a top priority as cybercriminals continue to develop new technologies to exploit vulnerabilities. This paper covers the complex world of cyber-attacks on computer networks, understanding their various topics and evolving strategies criminals' use.[2]

Drawing on intelligence, international law, and extensive research data, this article critically analyzes cyber threats and related countermeasures worldwide in recent years. It carefully identifies and highlights a variety of attacks, including malware, phishing, distributed denial of service (DDoS), ransomware, and insider threats, revealing their modus operandi and implications for organizations and individuals.

In addition, this article also covers the field of emerging cyber threats in the Internet of Things (IIoT) ecosystem and digital substations, highlighting vulnerabilities in the sector: 4.0 standard and distributed hardware and software architectures. difficult. This article highlights the importance of cyber defense and effective security strategies by revealing evolving challenges.[2]

Combining research findings and recommendations, this study aims to provide participants with insights and tools to strengthen cybersecurity. The recommendations include a range of measures, including enhanced threat detection capabilities, strong authentication mechanisms, stringent encryption protocols, and an employee training program.

Finally, the entire purpose of this study is to promote a deeper understanding of the various cyber threats and vulnerabilities in computer networks. This article aims to support efforts to reduce cyber risks and increase the impact of digital processes on environmental threats by providing stakeholders with information and effective strategies.[2]

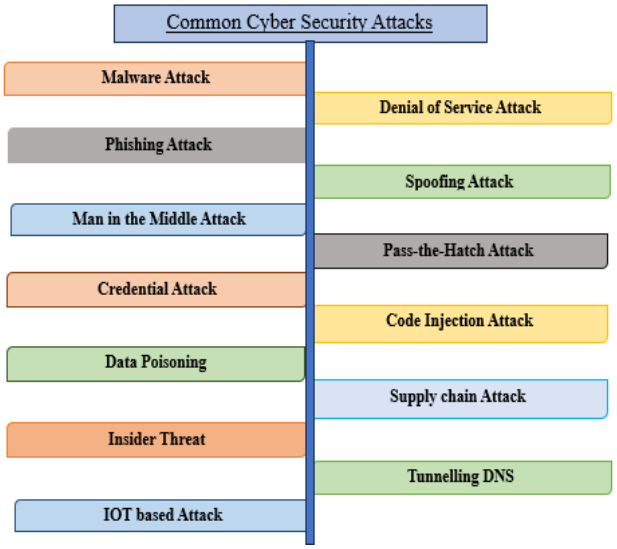
II. CYBER THREATS

Cyber threats are intentional attacks that involve unauthorized access to a network or sensitive data, often resulting in the destruction, corruption or theft of IT assets. These attacks, carried out by individuals or organizations, are carried out by exploiting vulnerabilities in computer systems and networks. They cover a wide range of crimes, from malware to denial of service to theft and fraud. As daily life becomes more dependent on technology, cybercrime has become a serious problem for individuals and organizations. These computer and internet-related crimes pose a serious risk to data security and privacy. General understanding. This lack of understanding can hinder efforts to prevent these threats. Although terms such as cyberattack and cybercrime have different meanings, they share the goal of compromising the privacy, integrity, and availability of information. Technological advances continue to push cybercrime forward, leading to new attacks and making prevention increasingly difficult. However, traditional cyber threats remain the most common form of attack, demonstrating the continued need for cybersecurity measures.[3]

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 11 Issue 6 June 2024



III. TYPES OF ATTACKS IN CYBERSECURITY

1. Malware:

Malware is a common threat in the digital world and includes a variety of malicious software specifically designed to cause serious damage to a computer, network or server. There are many types of malwares, from ransomware to Trojans, spyware to viruses, worms to keyloggers, and they all pose risks to cybersecurity. These malicious programs are created and used by cyber attackers for a variety of motivations, from surveillance to financial gain. Their undercover work often revolves around obtaining appropriate credentials and accessing sensitive information without the user's knowledge. As a result, malware attacks are still a threat that has the potential to cause serious harm to people, businesses, and entire systems [4]

Types of Malwares

Ransomware: In a ransomware attack, the attacker encrypts the victim's data and offers a decryption key in exchange for payment. Ransomware attacks are often reported via malicious links sent in phishing emails, but they can also be used without a malicious or illegal purpose. Native legal tools used to carry out ransomware attacks. Unlike traditional malware, fileless malware does not require attackers to install any code on the target, making it difficult to detect. Collecting information about website users without permission.[4]

Adware: It is a type of spyware that monitors the user's online activities to determine which ads to display to the user. Although adware is not malicious, it can affect the functionality of the client and disrupt the user experience.

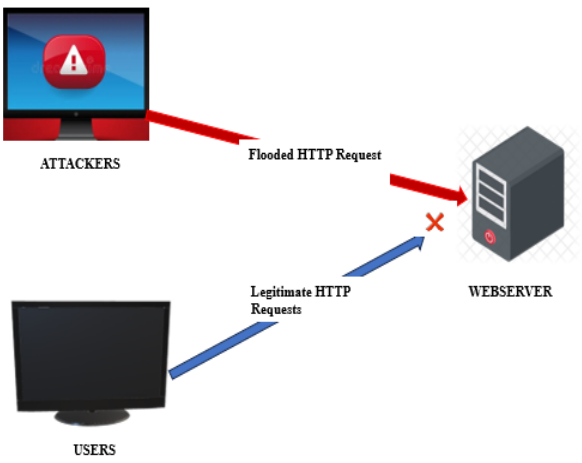
Trojan: A Trojan horse is a type of malware that masquerades as legitimate software, program, or harmless information (such as a free download). Trojans are installed through social engineering such as phishing or booby-trapped websites. Zeus Trojan malware is a strain that targets financial information and embeds systems into botnets.

Botnets: A botnet is a network of malware-infected computers controlled by zombies. An attacker is someone who operates a botnet infrastructure and uses infected computers to launch attacks designed to compromise the target network, inject malware, obtain credentials, or perform intense CPU usage. Emails containing malicious content such as viruses or malware as malicious payloads are classified as malware.

Worms: A virus is an independent program that can replicate itself and spread copies of itself to other computers. Viruses can infect the target through malware or can be sent via phishing or text messages. Embedded worms can modify and delete files, inject more malware, or infect sites until the target runs out of resources.

Rootkit: Rootkit malware is a collection of software that allows malicious actors to gain control of a computer network or application. While the malware is running, it creates external vulnerabilities and can infect other malware. Bootkit goes one step further and distributes critical boot files before the operating system starts, sometimes invisibly.[4]

2. A Denial of Service (DoS) attack:



A DoS attack is designed to disable a computer or network so that legitimate users cannot access it. This is done by distracting the target with excessive traffic or causing an accident. Therefore, users (such as employees, members, or account holders) cannot access services or resources. High targets often include websites of banks, business centers, media companies or government agencies. Although DoS attacks are not directly related to data theft, they cause financial and time loss to victims. These attacks generally occur in two ways: service interruption or resignation. In a flood attack, the system is overwhelmed with more traffic than it can handle, slowing the system down or shutting it down completely.[4]

Buffer overflow attack - The report of the DoS attack caused the target to be flooded with more traffic than it could handle. This includes many policies, including specific plans or network protocols.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 11 Issue 6 June 2024

ICMP Flood - pinging attacks all computers on the target network by sending fake packets instead of malicious packets. The network is a private network. machine. The network is then built to expand the traffic. This attack is also called cute attack or death ping. Continue until all open ports are filled with requests and there are no ports left for legitimate users to connect to.

SYN Flood - A request to connect to the server is sent, but the handshake is never completed. Connect until all open ports are filled with requests and there are no more ports left for legitimate users to connect to.

3. Phishing Attack:

Phishing is a type of cyberattack that uses email, text messages, phone calls, social media, and social engineering techniques to trick victims into sharing sensitive information (such as passwords or account numbers) or downloading malicious files and placing them on their computers. Or there is a virus on the phone.[4]

Common phishing attacks include:

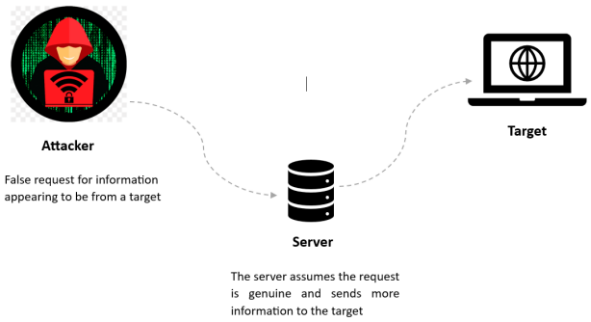
Spear phishing targets individuals or organizations through malicious emails, aiming to steal sensitive data like login credentials or install malware on the victim's device.

Whaling attacks are social engineering attacks focused on high-ranking executives, intending to extract money, sensitive information, or facilitate further cyber threats.

SMiShing scams use fake text messages to deceive individuals into divulging sensitive details like passwords, usernames, or credit card numbers, often by impersonating legitimate entities such as banks or shipping services.

Voice phishing, or vishing, involves fraudulent phone calls and voicemails from seemingly reputable organizations, aiming to trick individuals into disclosing personal information like banking details and passwords.[4]

4. Spoofing:



Spoofing is the process by which cybercriminals disguise themselves from a known or trusted source. By doing this, the attacker can communicate with the target and gain access to their system or device, with the primary goal of stealing data, downloading money, or installing malware or other malware on the device. These include:

Kerberoasting: Kerberoasting is a post-attack technique in which the attacker impersonates a user account with a principal domain name (SPN), requests a ticket or kerberos with the encrypted password, attempting to crack the password of a service account in Active Directory (AD).[4]

5. Man in the Middle (MITM) Attack:

Man in the middle is a cyber attack in which an attacker eavesdrops on conversations between two targets with the aim of collecting personal information, passwords or details at the bank and/or forcing the victim to take an action such as changing their ID card. Complete a transaction or initiate a refund. encourage.[4]

6. Pass-the-Hatch Attack (PtH)

A Hatch Traversal Attack is a type of attack where an attacker steals a "hash" of user information and uses it to create new user sessions on the same network. The attacker does not need to know or crack the password to gain access to the system. Instead, it uses the saved password to start a new session.[4]

7. Credential Stuffing:

Anti-object attacks are based on the assumption that people often use the same user ID and password across multiple accounts. Therefore, having a certificate for one account can grant access to another account. This prevents account lockouts, which typically occur when an attacker tries to compromise an account by trying multiple passwords. Brute force attacks: Brute force attacks use trial and error to determine high-access data, certificates, and encryption keys.[4]

The attacker sends the username and password together until they finally guess the correct one.

8. Code Injection Attacks:

An attacker can change the behavior of a computer or network by injecting malware. This process is called code injection. Vaccines can be used in many ways.

SQL Injection Attack: SQL Injection Hackers can exploit system flaws to inject malicious SQL queries into the database and use SQL injection to extract information from the database. Hackers use SQL injection to modify, steal or delete database information in an application.[4]

Cross-Site Scripting (XSS): Cross-site scripting is an injection technique in which attackers inject malicious code into legitimate websites. The code then spreads malicious code to the user's website, allowing the attacker to steal

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 11 Issue 6 June 2024

sensitive information or harm the user. Online forums, forums, blogs, and other websites that allow users to post their own content are often vulnerable to XSS attacks.

Malvertising: Malvertising attacks use many other tactics, such as organic SEO, to attack themselves. Attackers often infect other servers first, which allows cybercriminals to inject malicious code into ads or specific elements of ads, such as banner ads, creator images, or video content. When a website visitor clicks on an ad, the error code in the ad can install malware or adware on the user's computer.

9. Data Poisoning:

Data poisoning is a type of cyberattack in which an attacker intentionally breaches data using artificial intelligence or machine learning models to control the performance of the model. When checking data during processing, attackers can introduce biases, intentionally create artifacts, introduce flaws, or impact the model's predictive capabilities.[4]

10. Supply Chain Attack:

A hacking attack is a type of cyber-attack that causes third parties to compromise services or software that are important to the device. While software provides a chain of custody that prevents malicious codes from being injected into the application and infecting all users of the application, hardware provides a chain of custody that prevents tampering with the body for the same purpose. Customized software products are especially easy because modern software is not only written from scratch, but also includes many off-the-shelf products such as third-party APIs, open-source code, and rights provided by the software vendor.[4]

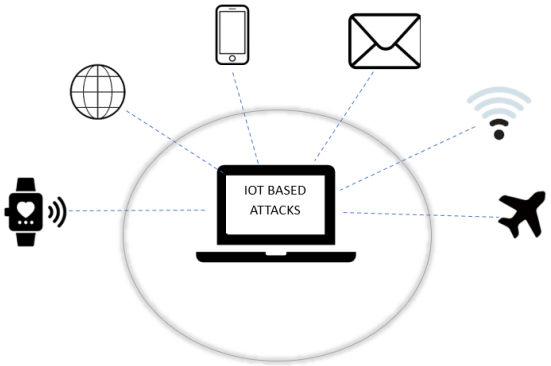
11. Insider Threats:

IT teams focused on finding candidates outside their own organization only know half the story. Insider threats are internal actors, such as current or former employees, who pose a threat to the organization because they have direct access to partners, sensitive information, and intellectual property (IP), including business information, regulatory rights, or others. This information will support the attack. Some of these motivations include selling confidential information for money on the dark web and/or using social engineering tactics such as social anxiety attacks, marketing copy email interception (BEC) attacks, or disinformation campaigns as a pretext. On the other hand, some threats from actors are careless rather than malicious in nature. To solve this problem, organizations need to implement a cybersecurity awareness program that informs stakeholders about all possible attacks, including those that can be carried out by insiders.[4]

12. Tunneling DNS

DNS tunneling is a network attack that uses DNS queries and responses to send code and information across the network, bypassing normal security measures. Once the hacker gains access, he is free to perform command and control operations. Tunneling slowly adds information to DNS responses, allowing hackers to inject malware and/or extract data, IP addresses, or other sensitive information. Attacks using DNS tunneling have become more common in recent years, in part due to ease of deployment. Even easily accessible tunneling toolkits and instructions can be found online on popular sites like YouTube.[4]

13. IoT Based Attacks



IoT attacks are cyber-attacks that target Internet of Things (IoT) devices or networks. Once compromised, hackers can take control of a device, steal data, or join a group of infected devices to form a botnet to launch a DoS or DDoS attack. One in 10 mobile phone infections originate from these devices; This is more than double the figure in 2019. Additionally, the deployment of 5G networks will encourage the use of expanded equipment and may also increase the number of attacks [4][10][11]

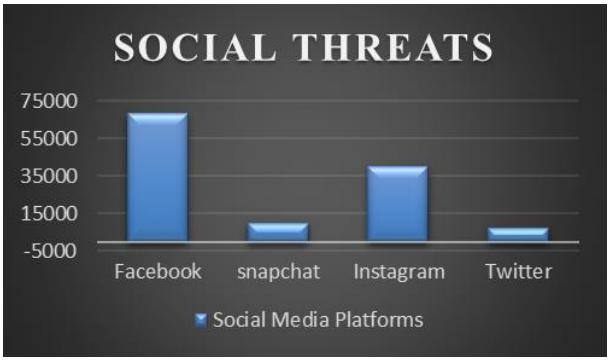
IV. ROLE OF SOCIAL MEDIA IN CYBER SECURITY

Social media has become an important part of life today. Approximately 4.8 billion people worldwide make up 59% of the world's population. Although social media is a powerful tool for connecting people and organizations, fostering relationships and sharing ideas, it also presents significant privacy and security challenges. The success of social media has led to online threats that users need to be aware of. One of the most important security concerns is the risk of malware. Due to the interactive nature of social media, users will often click on links without proper analysis, potentially exposing themselves to malware or phishing threats. This vulnerability provides a great opportunity for cybercriminals to launch attacks and gain unauthorized access to personal information, causing financial loss or celebrity damage.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 11 Issue 6 June 2024



Social media platforms also offer activists the opportunity to gather information about social media attacks. By impersonating a trusted person or organization, cybercriminals can trick users into revealing sensitive information such as passwords or financial details. These types of attacks are particularly dangerous because they exploit users' trust in social networks, making them vulnerable to fraud.

The amount of information shared on social media can also be overwhelming for users. People often provide personal information, photos and videos that can be used to create content for attacks. This combination can be detrimental to business and personal security, as attackers can use this information to improve their strategies and increase their chances of success.

Despite these risks, social media can play an important role in improving online security. Many platforms are investing more in security measures, such as machine learning algorithms that detect suspicious activity and prevent the spread of malware. Additionally, social media can be an important tool for online security awareness and educating users on best practices for protecting themselves online.

The influence of social media also enables the rapid dissemination of information about emerging threats, allowing

organizations and individuals to respond quickly and minimize

damage. By using social media as a platform to share information and collaborate on cybersecurity measures, professionals can work together to develop effective strategies and tools to combat cyber threats.

As social media continues to evolve, users need to ensure online security. This includes regularly updating the privacy

policy, being wary of suspicious messages and links, and understanding the latest trends in cyber-attacks. By

balancing social benefits with a strong commitment to sustainability, individuals and organizations can benefit from the connections and opportunities provided by the platforms while minimizing cyber risk.[5]

V. STEPS FOR PREVENTION OF ATTACKS:

Update software: Software Updates can fix any bugs and vulnerabilities in the software; so, having the latest version is your best bet. Also consider investing in a managed environment to keep your software up to date.

Set up a firewall.

Backdoors and denial-of-service assaults are two types of attacks that firewalls can assist avoid. They function by managing the network traffic that passes via your system. Additionally, a firewall will halt any unusual behavior that it determines could endanger the system.

Make a backup of your data.

Data backups involve moving the data to a different, safe location for storage. This could entail using a physical device, such as a hard disk, or cloud storage. Having a data backup enables you to retrieve any lost information in the event of an attack.

Encrypt information: Data encryption makes sure that only people with the decryption key can access data, making it a popular method of preventing cyberattacks. It is difficult to break encryption because attackers frequently have to use the brute force technique, which involves attempting a variety of keys until they figure out which one works, to successfully attack encrypted data.

Make secure passwords: To thwart assaults, you should create strong passwords and refrain from using the same ones across several platforms and accounts. Repetitively using the same password raises the possibility of providing hackers with complete access to all of your data. You can keep your accounts safe by changing your passwords on a regular basis and creating passwords that combine capital and lowercase letters, numbers, and unusual characters.[6]

VI. CYBERSECURITY CHALLENGES THAT INDIA IS FACING

As digital infrastructure expands, India faces various cybersecurity challenges, including major incidents and ongoing threats. For example, the country has seen an increase in cybercrime such as phishing attacks and ransomware. In 2021, the Indian government and companies faced ransomware attacks against organizations such as the National Health Service and Jindal Steel, compromising critical information and disrupting services.

Increasing reliance on mobile devices puts millions of users at risk from malware, including apps that can steal personal information or damage devices. For example, a popular Indian mobile application was found to have a vulnerability that attackers could exploit.

In 2020, the Bank of India reported an increase in cyber fraud cases in the banking sector, emphasizing the need for more security measures in the financial sector may affect the ability to respond effectively to emerging threats. This flaw is further exacerbated by the country's digital economy and e-commerce, and cybercriminals aim to financially gain from this vulnerability. For example, online retailer Flipkart faced a data breach in 2021 that exposed customers' personal information.

India’s Data Protection Act is yet to be enacted, leading to

differences in privacy laws. It can also invest in cybersecurity training and workforce development to create professionals who can protect against cyber threats.[9]

Advantages of Cyber Security

- Protect personal data
- Help protect reputation
- Improve productivity
- help remote working Compatibility
- Improve network conditions
- Better data management
- Helps train and train employees
- It helps maintain trust and confidence
- Provides easy access control
- Supports IT team [2]

Disadvantages of Cyber Security

- Regular Update
- Needs Continuous Learning
- Complex to Setup
- Slower System
- Constant Monitoring
- Talent Shortage
- Expensive [2]

VII. CONCLUSION

In short, network security involves countless attack vectors, and social media plays a significant role in today's threats. Measures such as strong authentication processes and regular security updates are important to reduce risk. However, India faces unique challenges such as infrastructure deficiencies and shortage of experts in cybersecurity. Despite these challenges, investing in cybersecurity has many advantages, such as protecting sensitive data and protecting critical systems. However, there are also some disadvantages that can hinder innovation, such as overregulation. Solving these complex problems requires a multifaceted approach that combines technology with regulatory frameworks and international cooperation to create a sustainable cybersecurity ecosystem

REFERENCES

[1] Tushar P. Parikh et al. “Cyber security: Study on Attack, Threat, Vulnerability” International Journal of Research in Modern Engineering and Emerging Technology Vol. 5, Issue: 6, June: 2017 (IJRMEET) ISSN: 2320-6586.

[2] Sheth, Mrs. & Bhosale, Sachin & Kurupkar, Mr. & Prof, Asst “Research Paper on Cyber Security” contemporary research in india (issn 2231-2137): special issue: April, 2021

[3] Gade, Nikhita Reddy & Reddy, Ugander. (2014) “A Study of Cyber Security Challenges and Its Emerging Trends on Latest Technologies”.

[4] Crowdstrike: (10 Most Common Types of Cyber Attacks) https://www.crowdstrike.com/cybersecurity-101/cyberattacks /most-common-types-of-cyberattacks/

[5] Kalakuntla, Rohit & Vanamala, Anvesh & Kolipyaka, Ranjith. (2019). “Cyber Security”. Holistica. 10. 115-128. 10.2478/hjbpa-2019-0020.

[6] Leaf-it: (10 Ways to Prevent Cyber Attacks) https://leaf-it. com/10-ways-prevent-cyber-attacks/

[7] Aslan, Ö.; Aktu˘ g, S.S.; Ozkan-Okay, M.; Yilmaz, A.A.; Akin, E “A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions.” Electronics 2023,12, 1333. https:// doi.org/10.3390/electronics12061333

[8] Jibi Mariam Biju1, Neethu Gopal2, Anju J Prakash3 “Cyber Attacks and Its Different Types” International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 06 Issue: 03 | Mar 2019

[9] Atul Arun Patil, “Research Paper on Cyber Security Challenges and Threats” International Journal of Advanced Research in Science, Communication and Technology (IJARSCT) ISSN (Online) Volume 4, Issue 1, January 2024

[10] Javapoint: (Types of Cyber Attacks) https://www.javatpoint. com/types-of-cyber-attacks

[11] Swimlane: (Types of Cybersecurity Attacks) https://swimlane. com/blog/types-of-cyber-security-attacks/