SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY

IT2030 - FINAL REPORT

Group 16 - Cyber Attacks

Authors:
Hoang Long Vu
Hoang Gia Nguyen

Student ID:
20204897
20204889

Jan 2021

Contents

Abstract

This report represents some basic definitions related to Cyberattacks and provides an overview of the history and the evolution of Cyberattacks over the years. Moreover, based on the current statistics of Cyberattacks along with a brief analysis of the operations and targets that some of the most common Cyberattacks aim to, we introduced various basic methods that every individual can implement to protect themselves from Cyberattacks on the Internet.

1 Introduction

Industry 4.0 has introduced the most significant innovations across all the fields. However, the state-of-the-art technology provided by Industry 4.0 has facilitated the attacks to conduct the most sophisticated and devastating Cyberattacks in recent years. Many companies, businesses, organisations, or even the government are suffering thousands of Cyberattacks every day. As a result, millions of data leaked, and billions of dollars have gone up in smoke. Even worse, the COVID-19 pandemic has triggered various new motivations and methods for the attackers to carry out their Cyberattacks. This report is intended to provide the most basic information on Cyberattacks, in terms of technology, motivations, and a brief overview of the evolution of Cyberattacks over the years. Moreover, the report introduces the most common types of Cyberattacks, how these attacks work and who are the ideal targets. Based on that, various basic methods are presented, and every individual can easily implement those to protect themselves on the Internet.

2 What is a Cyberattack?

A *cyberattack* is any offensive manoeuvre that targets computer information systems, computer networks, infrastructures, or personal computer devices.[1]. People that carry out cyberattacks are generally regarded as *cybercriminals*, and the products that facilitate a cyberattack is sometimes called *cyber weapon*.
Depending on the context, cyberattacks may be considered part of *cyber warfare* - which involves the actions by a nation-state or international organisation to attack and attempt to damage another nation's computers/networks.
A cyberattack may steal, alter, or even destroy a specified target. The motivations behind cyberattacks can vary, including [2]

- Political: Hackers tend to express their hatred or criticism towards the governments, or society, through cyber attacks. These cybercriminals may try to crash governmental websites, usually with the DDoS technique (all the mentioned techniques in this section will be discussed in detail later). By VNCERT, there were about 3.3 million infected IPs, over 18,000 websites were manipulated by cybercriminals, including 88 government websites in 2015.[3]

- Financial: This is the most likely reason an organisation can get attacked. Cybercriminals may try to steal money from financial accounts, stealing credit card credentials from users. Furthermore, hackers may cause data branches resulting in the collapse of many companies.

- Business competition: DDoS attacks are increasingly being used as a competitive business tool. Cybercriminals may prevent business competitors from hosting/participating in major events, or may even shut down an online business for months. As a result, those businesses will suffer from severe financial and reputation damage.

On the other hand, cyberattacks are not always about bad things. One common good application of Cyberattack is the *penetration test* (pen test). Generally, a pen test is an authorized simulated cyberattack on a computer system, conducted to evaluate the security of a system. The primary goal of pentest focuses on finding *vulnerabilities* that could be exploited by any other threats, therefore the organisation can take the initiative in carrying out security methods for their systems.

However, cyberattacks can not just happen out of nowhere. Three fundamental factors that contribute to any Cyberattack are the fear factor, spectacularity factor, and vulnerability factor.

- The *spectacularity* factor relates to the damage that can be achieved by the malicious attacker. As mentioned above, the damages may include a drop in publicity of the victim/business, as well as loss of income of an organization/individual.
- The *fear* factor implies an attacker's intention to instil fear in their victims. *Ransomware* attacks are a good example of the fear factor being utilized by the malicious party to get what they want from the victim
- The next factor relates to the *vulnerability* of an organisation or individual. Since some companies might be using outdated security systems and infrastructure, this makes them an easy target for attackers. Therefore, companies must carry out regular penetration tests to discover any vulnerability as soon as possible.

3 History of Cyber Attacks

In this section, let's wind back through the timeline to have a closer look at some notorious Cyberattacks in history. The first cyberattack is believed to date back to the 1830s, when the *Blanc brothers* hacked the French Telegraph System and succeeded in stealing confidential financial market information. However, the brothers could not be convicted on trial because there was no law against the misuse of data networks in France.

Robert Tappan Morris, son of Robert Morris - a former cryptographer at NASA, created one of the first *computer worms* on the Internet in 1988, when he was a graduate student at Cornell University. An Internet worm is a type of malicious software (*malware*) that self-replicates and distributes copies of itself to its network. Morris was just curious about the Internet and had no intention for the worm to be such actively destructive. The Morris worm was estimated to rapidly infect 6,000 machines connected to the internet, depleted of their resources and even shut down the machines. This is also known as the first widespread cyberattack and the first *Distributed Denial-of-service* (DDoS) attack in history. The total damage was estimated to be around 10 million dollars and caused him to be sentenced to three years of probation.

Ransomware is a type of malware that threatens to publish the victim's data, or perpetually block access to it unless a ransom is paid. Advanced malware adopts a technique called *cryptoviral extortion* (using cryptography to design powerful malware) with the main goal of encrypting the victim's file. Therefore, the victim needs to pay the hackers to decrypt their files for accessibility. One of the most destructive worldwide ransomware attacks is *WannaCry*, which happened in May 2017. The attack was targeted at Windows computers, and despite Microsoft having quickly released patches to close the exploit, much of WannaCry's spread was from organisations that had not applied those latest updates. The victims are demanded to pay with Bitcoin cryptocurrency for their data decryption. The WannaCry cyberattack was estimated to have affected over 200,000 computers across

150 countries with a total cost of around 8 billion dollars!

Malware is adopted by a host of notorious attacks due to its severe destructibility, and the most costly cyber-attack ever also implemented this malicious software. *Petya* - firstly discovered in 2016 - was a malware that targets Windows-based systems, could encrypt hard drive file systems and prevent Windows from booting. Similarly, the victims are demanded to make a payment in Bitcoin to regain access to the system. The *NotPetya* variant was used later in 2017 and was confirmed by the White House that the total cost was estimated at 10 billion dollars, which makes it one of the most costly cyberattacks in history.

However, cyber-attacks do not always originate from individuals or private groups. Approximately 120 countries have been developing ways to use the Internet as a weapon and target financial markets, government computer systems and utilises. As mentioned above, Cyberattack may be a part of cyber warfare, and with the emergence of cyber as a substantial threat to national and global security, cyberwar, warfare and/or attacks also became a domain of interest and purpose for the Military. In 2008, Russia began a cyber attack on the Georgian government website, which was carried out along with Georgian military operations in South Ossetia. In the same year, Chinese "nationalist hackers" attacked CNN (a television channel based in the US) as it reported on Chinese repression on Tibet *(a traditional homeland to an East Asian ethnic group).*

4 Evolution of cyber-attacks

The idea in this section was referenced from the paper: *Overview of Cyber Security in the Industry 4.0 Era*, Beyzaur Cayir Ervural, Bilal Ervural.[4]
The cyberattack techniques are constantly altering and evolving due to the tremendous growth of technology, the complexity of the attackers, the value of potential targets and the effects of attacks.With the widespread use of computer networks, hackers have taken advantage of network-based services to gain personal benefit and reputation.Each organization has digital knowledge and many businesses maintain business transactions and trades with online systems. Most enterprises are open to cyber threats attacking from external and internal boundaries. Therefore, it is a must that the critical infrastructure is under strict supervision against any type of cyberattack.

Cyber security was initially seen as a problem for the IT team, but these days it is *an agenda for the entire senior executives.* Cybercrime is triggered by sophisticated technologies, the use of mobility, social media, and relatively new trends in rapidly expanding connectivity—all in the hands of organized criminal networks. Under these circumstances, a smart, dynamic and evolutionary approach to cyber security is crucial to stay ahead of cybercrime and competition. Cyber security efforts require protection against a broader range of challenges. It is getting harder with new technologies, trends in mobile usage, social media, well-financed and organized enemies and 24-h attacks. Cyber risks can have a direct impact on everything from stock exchange price to brand reputation, with their more complicated structures.

Figure 1 shows how cyber-attacks have evolved over the years and what industry will see in the coming years *(Frost and Sullivan 2017).*

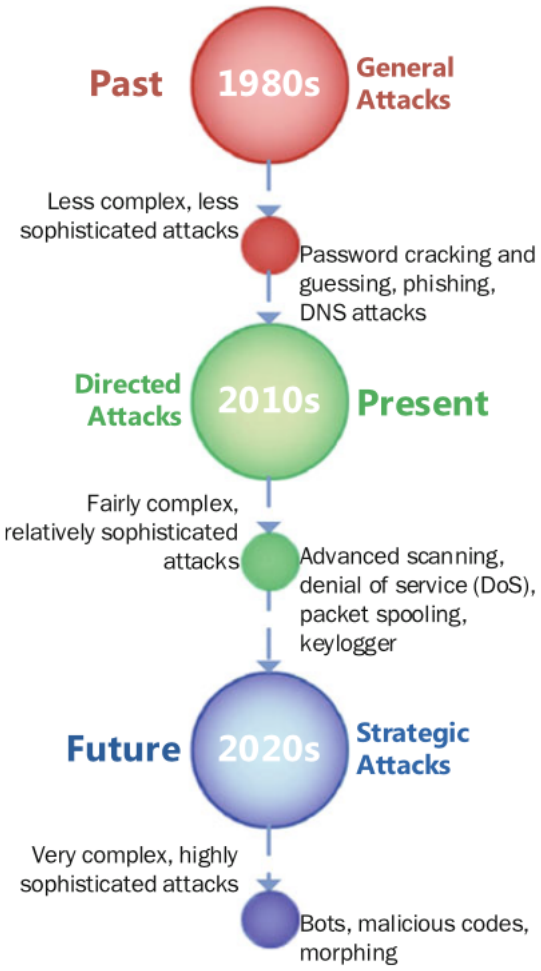

Figure 1: The evolution of Cyberattacks

Over time, the nature of cyber-attacks has been complicated and extremely sophisticated. At the beginning of the 1980s, general cyber-attacks began with password cracking and password guessing methods. Today, directed cyber-attacks occur with packet *spooling*, advanced scanning, *keylogger* and denial of service. In the future, strategic cyber-attacks are expected to damage strategic points with bots, morphing and malicious codes.

5 The current trend of cyber-attacks

Cybercriminals are constantly evolving with considerable improvements in the technology, tools, methods used to carry out cyberattacks. In this section, let us have a quick overview of the latest trends in Cyberattack.

5.1 Remote working risks

The COVID-19 pandemic forced most businesses, organisations, or even schools to switch to remote and online learning/working. However, this situation poses new cybersecurity risks as home offices are often less protected than centralised offices (which are deemed to have more secure firewalls and strict access management maintained by professional

IT security teams). A recent survey from the UK and US-based security firm, Tessian, found that 56% of senior IT technicians believe their employees have picked up bad cyber-security habits while working from home. To take as an example, the BBC reported that In November 2020, a Sydney-based hedge fund collapsed after a senior executive clicked on a fraudulent Zoom invitation. The company - Levitas Capital - reportedly lost 8.7m USD to the cyber-attack and was forced to close. [5]

5.2 The evolution of the Internet of Things (IoT)

On one hand, it is undeniable that IoT is an out exceptional and important innovation in Industry 4.0. IoT refers to physical devices other than computers, phones, and servers, which connect to the Internet and share data. Thanks to IoT solutions, mundane tasks can be done automatically, thus reducing the costs of business operations. Moreover, the is a host of different applications of IoT to many extents, including: connecting devices and people, improving customer experience, etc.

On the other hand, the expanding IoT creates more opportunities for cybercrime. Kaspersky reported that there has been 1.51 billion breaches of IoT devices from January to June 2021. Moreover, some 16 "large scale" data leaks occurred in Vietnam over the reporting period, according to local media outlet VnExpress International. Compromised IoT was cited as one of the major contributing factors.

5.3 The rise of ransomware

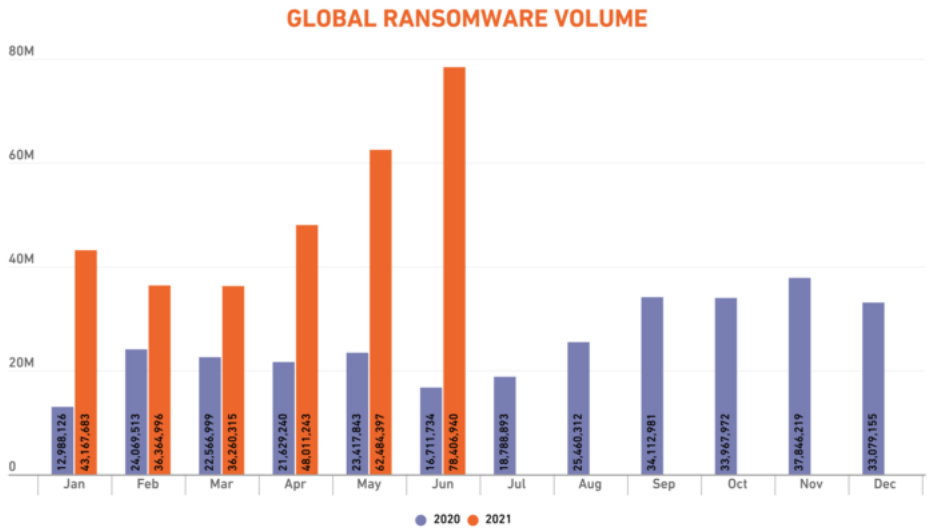

Figure 2: Total ransomware volume (by *SonicWall*)

As aforementioned, ransomware is a powerful method for the most destructive Cyberattacks. Ransomware attacks surged 93% in the first 6 months of 2021 as seen in the Figure 2, fueled by an innovation in attack technique called *Triple Extortion*. Every week, more than 1,200 organisations worldwide fall victim to a ransomware attack, and all enterprises are at risk. The average ransom payment increased by 171% during the past year and is now approximately 310,000 USD. Over 1,000 companies suffered data leakage after not giving in to ransomware demands during 2020. Furthermore, it is daunting that attackers are still seeking methods to improve their ransom payment statistics, and their threat efficiency.

5.4 Phishing

Phishing involves a malicious actor impersonating a trustworthy entity to obtain private data. Such attacks can be carried out via emails, websites, or other means. Attackers can either trick victims into providing sensitive information — such as credit card information or passwords — or downloading malicious attachments.

- 38% of cyber attacks on US companies involve phishing.
- 38% of end-users, up from 8.3% in 2019, without cybersecurity awareness training, will fail phishing tests.
- Google detected around 2 million phishing sites in 2020.
- According to the 2020 Mobile Threat Landscape Report, a new phishing site is launched every 20 seconds.
- About 5% of all emails are phishing (*by Avanon, 2021*).

More than that, many attackers have taken advantage of the COVID-19 Pandemic to impersonate their phishing emails as important pandemic news. It is not always easy to recognise the email below as a phishing threat.

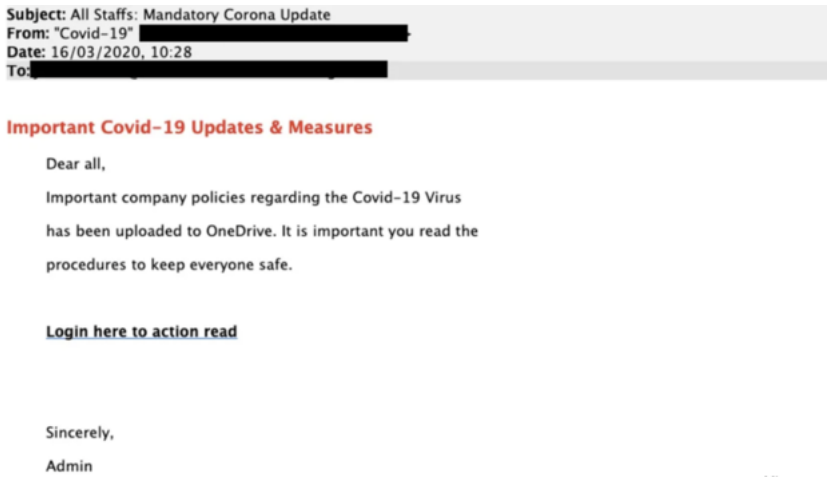

Figure 3: A phishing email

Therefore, we should raise our awareness of every piece of information we receive nowadays and implement necessary methods to protect ourselves against cybercriminals. Further methods will be discussed in detail in **Section 6** of this report.

6 Consequences

There is no doubt that Cyberattacks can result in severe consequences, relating to numerous aspects in different fields. In this section, we will take a deeper look at the negative impacts of Cyberattacks.

6.1 Individuals

In terms of individual-scope impacts, Cyberattacks can lead to the loss of money or the theft of personal, financial and medical information. These attacks can damage the reputation, safety of organisations. More than that, the data collected illegally can be further used for:

- **Sell data:** user's data will be sold to the dark web and these collections can include millions of records of stolen data. The buyers can then use this data for their criminal purposes.
- **Identity theft:** Many online services require users to fill in personal details such as full name, home address and credit card number. Criminals steal this data from online accounts to commit identity theft, such as using the victim's credit card or taking loans in their name.
- **Account takeover:** Criminals use stolen login credentials to break into accounts with payment details, such as shopping accounts. This is called *account takeover*, and it often leads to identity theft. If the hacker changes your password, the user will also lose access to your account. Account takeover can be costly if the hijacked account includes payment details.

6.2 Organisations

Cyberattacks not only give consequences to an individual but also any organization. Specifically:

- **Reputational damage:** Loss of customer and stakeholder trust can be the most harmful impact of cybercrime since the overwhelming majority of people would not do business with a company that had been breached, especially if it failed to protect its customers' data.
- **Financial loss:** Cybercrime costs small businesses disproportionately more than big businesses when adjusted for organizational size. For a large corporation, the financial impact of a breach may run into the millions, but at their scale, the monetary implications are barely a blip on the radar. According to the latest data breach report by IBM and the Ponemon Institute, the average cost of a data breach in 2021 is 4.24M USD, a 10% rise from its average cost of 3.86M USD in 2019.
- **Fines:** As if direct financial losses weren't punishment enough, there is the prospect of monetary penalties for businesses that fail to comply with data protection legislation. In May 2018, the General Data Protection Regulation or GDPR went into effect in the EU. The enforcement powers associated with the law are significant. Fines for violations can reach up to 20 million Euros or 4% of a firm's global annual revenue, per violation, whichever is larger.

7 Common types of cyber attacks

There is a multitude of different types and techniques of Cyberattacks. However, this report will just enumerate some of the most common of Cyberattacks that everyone should be aware of.

7.1 Man-in-the-middle attack

A man in the middle *(MITM)* attack is a general term for when a perpetrator positions himself in a *conversation* between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway. The goal of an attack is to steal personal information, such as login credentials, account details and credit card numbers. Targets are typically the users of financial applications, e-commerce sites and other websites where logging in is required. Information obtained during an attack could be used for many purposes, including identity theft, unapproved fund transfers or an illicit password change. Broadly speaking, a MITM attack is an equivalent of a mailman opening your bank statement, writing down your account details and then resealing the envelope and delivering it to your door.
MitM attacks are one of the oldest forms of cyber attack. Computer scientists have been looking at ways to prevent threat actors tampering or eavesdropping on communications since the early 1980s. MitM attacks consist of sitting between the connection of two parties and either observing or manipulating traffic. This could be through interfering with legitimate networks or creating fake networks that the attacker controls. Compromised traffic is then stripped of any encryption to steal, change or reroute that traffic to the attacker's destination of choice (such as a phishing log-in site). Because attackers may be silently observing or re-encrypting intercepted traffic to its intended source once recorded or edited, it can be a difficult attack to spot.
Though not as common as ransomware or phishing attacks, MitM attacks are an ever-present threat for organisations. IBM X-Force's Threat Intelligence Index 2018 says that: 35 per cent of exploitation activity involved attackers attempting to conduct MitM attacks, but hard numbers are difficult to come by. In 2017 the Electronic Frontier Foundation (EFF) reported that over half of all internet traffic is now encrypted, with Google now reporting that over 90 per cent of traffic in some countries is now encrypted. Major browsers such as Chrome and Firefox will also warn users if they are at risk from MitM attacks. One example observed recently on open-source reporting was malware targeting a large financial organisation's SWIFT network, in which a MitM technique was utilized to provide a false account balance to remain undetected as funds

7.2 Distributed Denial of Service

A distributed denial-of-service *(DDoS)* attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices. From a high level, a DDoS attack is like an unexpected traffic jam clogging up the highway, preventing regular traffic from arriving at its destination.
DDoS attacks are carried out with networks of Internet-connected machines. These networks consist of computers and other devices (such as IoT devices) that have been infected with malware, allowing them to be controlled remotely by an attacker. These individual devices are referred to as *bots* (or zombies), and a group of bots is called a *botnet*. Once a botnet has been established, the attacker can direct an attack by sending remote instructions to each bot. When a victim's server or network is targeted by the botnet, each bot sends requests to the target's IP address, potentially causing the server or network to become overwhelmed, resulting in a denial-of-service to normal traffic. Because each bot is a legitimate Internet device, separating the attack traffic from normal traffic can be

difficult.
Some of the most commonly used DDoS attack types include:

- **UDP Flood:** A UDP flood, by definition, is any DDoS attack that floods a target with *User Datagram Protocol (UDP)* packets. The goal of the attack is to flood random ports on a remote host. This causes the host to repeatedly check for the application listening at that port, and (when no application is found) reply with an ICMP (*Internet Control Message Protocol*) 'Destination Unreachable' packet. This process saps host resources, which can ultimately lead to inaccessibility.

- **ICMP (Ping) Flood:** Similar in principle to the UDP flood attack, an ICMP flood overwhelms the target resource with ICMP Echo Request (*ping*) packets, generally sending packets as fast as possible without waiting for replies. This type of attack can consume both outgoing and incoming bandwidth, since the victim's servers will often attempt to respond with ICMP Echo Reply packets, resulting in a significant overall system slowdown.

Moreover, we can name some other DDoS techniques like: SYN Flood, Slowloris, Ping of Death, etc. However, the technical explanation is out of the scope of this report.

7.3 Spoofing

Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source. Spoofing can apply to emails, phone calls, and websites, or can be more technical, such as a computer spoofing an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server. Spoofing can be used to gain access to a target's personal information, spread malware through infected links or attachments, bypass network access controls, or redistribute traffic to conduct a denial-of-service attack. Spoofing is often the way a bad actor gains access to execute a larger cyber attack such as an advanced persistent threat or a man-in-the-middle attack. Successful attacks on organisations can lead to infected computer systems and networks, data breaches, and/or loss of revenue—all liable to affect the organisation's public reputation. In addition, spoofing that leads to the rerouting of internet traffic can overwhelm networks or lead customers/clients to malicious sites aimed at stealing information or distributing malware.
Spoofing can be applied to several communication methods and employ various levels of technical know-how. Spoofing can be used carry out phishing attacks, which are scams to gain sensitive information from individuals or organisations. The following different examples of spoofing attack methods gives more detail on how different attacks work.

7.4 Phishing

Phishing is a type of *social engineering* attack (the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes), often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information. An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identify theft. Phishing is often used to gain a foothold in corporate or governmental networks as a part of a larger attack, such as an advanced persistent threat

(APT) event. In the latter scenario, employees are compromised to bypass security perimeters, distribute malware inside a closed environment, or gain privileged access to secured data. An organisation succumbing to such an attack typically sustains severe financial losses in addition to declining market share, reputation, and consumer trust. Depending on scope, a phishing attempt might escalate into a security incident from which a business will have a difficult time recovering.
Some kind of phishing techniques:

- **Email phishing scams:** Email phishing is a numbers game. An attacker sending out thousands of fraudulent messages can net significant information and sums of money, even if only a small percentage of recipients fall for the scam. As mentioned above, the COVID 19 pandemic has unfortunately facilitate phishing hackers. Those cybercriminals can easily impersonate their malicious emails as important pandemic news, and thus tricked the victims into clicking the harmful address, or download the attachments in the email.

- **Spear phishing** Shortly, spear phishing targets a specific person or enterprise, as opposed to random application users. It's a more in-depth version of phishing that requires special knowledge about an organisation, including its power structure.

7.5 Malware

Malware, or malicious software, is any program or file that is intentionally harmful to a computer, network or server. Types of malware include computer viruses, worms, Trojan horses, ransomware and spyware. These malicious programs steal, encrypt and delete sensitive data; alter or hijack core computing functions and monitor end users' computer activity.
Malware can infect networks and devices and is designed to harm those devices, networks and/or their users in some way. Depending on the type of malware and its goal, this harm may present itself differently to the user or endpoint. In some cases, the effect malware has is relatively mild and benign, and in others, it can be disastrous. No matter the method, all types of malware are designed to exploit devices at the expense of the user and to the benefit of the hacker - the person who has designed and/or deployed the malware. Malware authors use a variety of physical and virtual means to spread malware that infects devices and networks. For example, malicious programs can be delivered to a system with a USB drive, through popular collaboration tools and by drive-by downloads, which automatically download malicious programs to systems without the user's approval or knowledge.
Phishing attacks are another common type of malware delivery where emails disguised as legitimate messages contain malicious links or attachments that deliver the malware executable file to unsuspecting users. Sophisticated malware attacks often feature the use of a command-and-control server that enables threat actors to communicate with the infected systems, exfiltrate sensitive data and even remotely control the compromised device or server.
Different types of malware have unique traits and characteristics. Types of malware include the following:

- A *virus* is the most common type of malware that can execute itself and spread by infecting other programs or files.

- A *worm* can self-replicate without a host program and typically spreads without any interaction from the malware authors.

- A *Trojan* horse is designed to appear as a legitimate software program to gain access to a system. Once activated following installation, Trojans can execute their malicious functions.
- *Spyware* collects information and data on the device and user, as well as observes the user's activity without their knowledge.
- *Ransomware* infects a user's system and encrypts its data. Cybercriminals then demand a ransom payment from the victim in exchange for decrypting the system's data.
- A *rootkit* obtains administrator-level access to the victim's system. Once installed, the program gives threat actors root or privileged access to the system.
- A *backdoor virus* or remote access Trojan (RAT) secretly creates a backdoor into an infected computer system that enables threat actors to remotely access it without alerting the user or the system's security programs.
- *Adware* tracks a user's browser and download history with the intent to display pop-up or banner advertisements that lure the user into making a purchase. For example, an advertiser might use cookies to track the web pages a user visits to better target advertising.
- *Keyloggers*, also called system monitors, track nearly everything a user does on their computer. This includes emails, opened webpages, programs and keystrokes.

8 Some basic methods to tackle Cyberattacks

Preventing and handling Cyberattacks may require some technical knowledge, and even experts are needed if the Cyberattacks are carried out at large scale to prevent devastating results. However, every one can apply the basic methods below to protect themselves from the Cybercriminals.

The first and most basic step in maintaining cybersecurity is to create a unique and original password for each account. Dave Hatter, a cyber security consultant at intrust IT, told Business Insider, "Unless you become aware of a password breach, there is no need to change your passwords regularly if each is a strong, unique password. This is even more true if you are using two-factor authentication." Users who change their passwords frequently end up taking shortcuts, and inadvertently make their passwords weaker and more easily hackable in the process. So users don't have to change the password every three months as suggested.

Keeping up with software updates is important, as cybercriminals often target known flaws in software to access a user's system. As mentioned in **Section 2**, keeping windows OS updated will prevent users from WannaCry. Operating system updates provide fixes to possible bugs and security holes, along with cleaning up outdated software that may slow down a user's device. Old and outdated software is vulnerable to hackers and cybercriminals as updates keep users safe from exploitable holes into user's organisations. Having reliable security in place is especially important as the release of software update notes often reveal the patched-up exploitable entry points to the public. Public knowledge of these holes leaves user's organisations easy prey for malicious users who are looking for a way to gain entry to user's business and its sensitive data.

Cybercriminals may comb through social media posts in search of information commonly used in security questions, such as a pet's name or mother's maiden name. To

combat this risk, social media users should set their account to private or avoid revealing sensitive information in posts. Victims increasingly accustomed to the warnings about phishing emails, yet phishing attacks happen plenty on social media. The same rules apply. Don't follow any links from strangers by way of instant or direct messengers. And keep personal information close. Don't pass out email, address, or other info as well. Even those so-called "quiz" posts and websites can be ruses designed to steal bits and pieces of personal info that can be used as the basis of an attack.

A virtual private network (VPN) is a great way to protect sensitive data, especially when accessing a public Wi-Fi network. A VPN encrypts all information transmitted by the user's device and helps prevent many types of cyberattacks. An IP address can be used to track victim's location and identity. Whenever a user visits a website, the website provider can see user's IP address, and may use that information in ad targeting in the future. However, using a VPN, user will be routing data through a VPN server with its IP address. Websites user interact with will only be able to view the VPN's IP address, and not their own. Everything you do online leaves traces that can tell a lot about your online habits. Many entities are trying to get data, ranging from the victim internet service provider (ISP) to online shopping websites. ISPs often snoop on their customers' data and can even pass it to third parties. For example, they can sell it to a governmental institution interested in what user do online or a commercial entity that may use it for marketing purposes or ad targeting.

Finally, teachers and parents should educate children about proper internet usage. Children and teens should know what the rules and guidelines are for surfing the internet and using social media. Malicious cyber activity affects students in a variety of ways, typically in the form of malware and scams. As students join classes this years using their personal computers and home wifi networks, the number of potential attack vectors has rapidly proliferated, according to Education Technology. Students, as one of the easiest target for hackers, should understand the dangers of cyberattacks to prevent themselves from such things.

9 Conclusion

It is undeniable that Cyberattacks are one of the most terrible threat on the Internet, for every individual, business, organisation, or even countries. Cyberattacks can cost billions of dollars and are becoming easier to implement than ever, thanks to the state-of-the-art technology provided by Industry 4.0. Phishing and ransomware are among the leading trends of Cyberattacks in recent years, and the IoT devices are becoming an ideal target for the cybercriminals. However, Cyberattacks are not inevitable as everyone can easily implement the most basic methods to withstand simple Cyberattacks. Simple tasks like keep the system updated, or changing passwords regularly may not take too much time, but appear efficient to protect ourselves on the Internet.

References

[1] Wikipedia contributors. Cyberattack — Wikipedia, the free encyclopedia, 2021. URL https://en.wikipedia.org/w/index.php?title=Cyberattack&oldid=1062060402. [Online; accessed 10-January-2022].

[2] https://lifars.com/2020/03/motivations-behind-cyber-attacks/. (Online; accessed 8-Jan-2021).

[3] https://cand.com.vn/Khoa-hoc-Quan-su/Tan-cong-mang-hien-dai-ngay-cang-\pha-hoai-tan-khoc-i372423/. (Online; accessed 8-Jan-2021).

[4] B.C.; Ervural Ervural. Industry 4.0: Managing the digital transformation. *Springer International Publishin*, 2018.

[5] https://www.news.com.au/technology/online/security/levitas-capital-closing-after-fake-zoom-invite-sinks-16m-super-fund-investment/news-story/1107504890205075589 21a95cbe2c980.