Malware and Type of Cyber Attacks Targeting Healthcare Industry

Vinesh Thiruchelvam, Reshiwaran Jegatheswaran, Daniel Mago Vistro
School of *Technology*
Asia Pacific University of Technology & Innovation
Kuala Lumpur, Malaysia
dr.vinesh@staffemail.apu.edu.my, TP038338@mail.apu.edu.my, daniel.mago@staffemail.apu.edu.my

***Abstract*— In the current era, technology has evolved into many industries. As the technology gets upgraded from time to time, the vulnerability of hardware and software do still exist and without proper action it may convert the vulnerability into a key for cybercriminals. Malware attack is the term that is usually being used to address attacks that are made towards individual computers. There are new types of malware attacks. These attacks are being made either to steal information or for ransom. Sometimes the attackers would just want to access the computer to gather credential and crucial information. On the other hand, there is also attackers who would want to make money whereby they would encrypt personal files or the computer and demand the individual to pay them a ransom in order to revert their actions.**

Keywords—Malware, Common Malware, Malware Timeline, Healthcare, Ransomware

I. INTRODUCTION

Malware is a collective name that is given for a number of malicious activities (Forcepoint, 2022). Malicious activity is a type of activity that is being conducted to bring an uneasy act for the users of the internet and technology. The effect of this activity sometimes could be severe, or they would be effectless. Out there in the world or internet, there are plenty of malicious activities. The organization that uses the technology and internet of things in their daily business operation are becoming the typical victims. The malicious activity is not only being done to the organization, but they are being conducted to individuals.

ELK Cloner is the very first computer virus that was discovered in the year 1982 (Landesman, 2021). Back then when the computer was developed the usage was low and the discovery of malware would take a longer time. Four years later the first PC- based malware was released and it was named 'Brain'. Earlier days the malware was simple whereby the attacks were made on the boot sectors or file infectors before the invention of a network. As networking became more prominent, the cyber attackers do not need to be present physically at the victim's machine, but they just need to use the network to begin malware attacks. When the network was being developed the security, level was weak. The attackers took that as an opportunity to implement attacks. This has increased the result of malware attacks in the first half of 1990s.

II. MALWARE IN 21ST CENTURY

As the network and technology improves and spreads into many industries and sectors, the usage and advancement of malware was also taking place that effected many individual users and organizations. With the help of the network development there were a significant increase in the late 1990's as malware attacks begin to spread via the emails (Kaspersky, 2022). The attackers spread the malware using emails to random users. Upon opening those emails, the malware will get activated. Time moved on, technology and network got more advanced and high-tech yet there is no full stop for the malware activity. In the 21 century the malware has become more advanced that the impact of it has destroyed hundreds of users' machines and millions of users' personal information has been disclosed to the public or being sold in the dark web for money. Figure below would provide a demonstration on the timeline of malware in the 21st century.

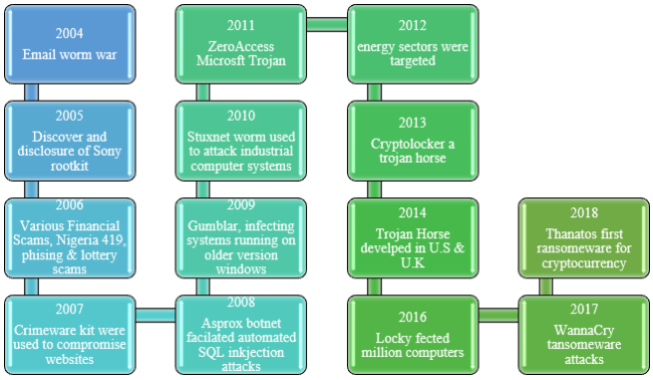


Figure 1 - Timeline of Malware for 21st Century (Landesman, 2021)

With the reference of Figure 1, a clear and understandable timeline is being displayed. We can understand that malware activity has gained its advancement in the 21st century. Every year there is always a new virus being introduced. The email worm war took place within authors such as MyDoom, Bagle and Netsky (Kaspersky, 2022). This action has resulted towards introducing an improved email scanning and higher adoption. Sony rootkit was used for the malware in 2005 (Milosevic, 2013). In 2006 various type of financial scams were seen, Nigeria 419, phishing, and lottery scams took place on the internet and causing a huge loss for the victims. In 2007, websites were compromised with the help of

crimeware. End of 2007 SQL injection had begun to be developed and in 2008 these SQL injections were used to attack the victim and one of the famous victims was Walmart.

After the older version used to attacke the industries became the victim to the Stuxnet worm in 2010 (Radware, 2022). The purpose of the attack was to attack the machinery of the factory. Years moved on, malware being introduced whereby in 2011, Zero Access a trojan horse, 2013 Crypto Locker another trojan horse were introduced. In 2016, Locky was used to infect several million computers in Europe using Disruptive Distributed DoS (DDoS) on various websites. In 2017 a malware was developed which brought the malware activity to another feal level on the individual users and industrial which is the WannaCry Ransomware attacks. This Ransomware has ended many users' machine and disclosed plenty of personal information on the internet world. During the mid of 2018, Thanatos was introduced. These attacks were conducted on Cryptocurrency as during that year the bitcoin became a hot topic that was being spoken about by many industries and sectors.

III. TYPE OF COMMON MALWARE

A number of malwares that occur frequently are Virus, Worms, Spyware, Trojan, and Ransomware. This lists of malwares are activities that happens almost every day. Each malware has its own purpose and impacts on the victims.

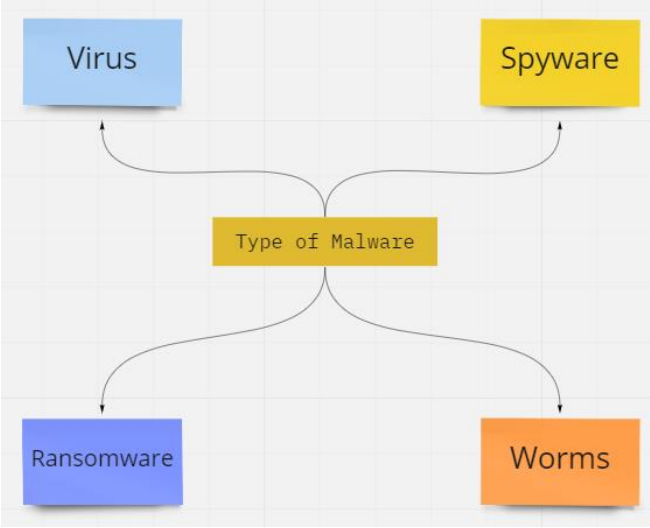


Figure 2 - The type of Common Malware Attacks (Mohammed N. Alenezi, 2020)

Figure 2 shows, the list of malware or malicious activities which is known to be the common attacks that have the current advancement of network and technology. The clear descriptions is as follows;

A. Virus

The term virus was first being discussed in a seminar in the

year 1983 (Vijayanand, 2019). Virus is defined as a program that is being attached with an application or other programs that is being downloaded by the users. The virus has its own capability to execute themselves when they are installed in a machine. The virus has the ability to copy their own code and infect the machine without the permission of the user. Basically, the hacker would input the virus program into the free program or application that is frequently being installed by the users. Upon being downloaded and being installed they will begin to execute themselves. This is where they will attack the machine or devices. The outcome of them executing themselves is that the machine of the user will begin to face slow performance, unexplained data loss and frequent machine crashing. Throughout the years, the number of viruses has increased and from time-to-time new viruses has been introduced (Milind J. Joshi, 2013).

There are many ways the virus could be spread to the machine of the victim, normally via networks, discs, email attachment or external storage devices (Webroot Inc, 2022). In the older days network connection was not a famous activity. Nowadays, the virus is being spread through network connections as the network connectivity plays a more vital role and almost all devices will need to access the network in order to use the internet.

There are three common methods a virus could be spread (Omoth, 2021). Firstly, infected email attachment. Speaking of email, the words does not carry the virus but if those emails do come with an attachment or links then those are the methods for the virus. When the user clicks the link or downloads the attachment the virus will execute themselves and begin the attack on the machine. When a user receives the email and clicks on it without any knowledge, they will download it and later the virus will execute in the user's computer causing a certain amount of effect.

Secondly, Removable Media. When we hear the term removable media it would indicate an external device. External devices here are such as the USB, External hard disk and more. One would wonder how the virus could get into the victims' machine? Out there in the in the public, there are hundreds of hackers waiting for their opportunity to discover weakness in the users' machine. The hackers will input virus into programs or files in the external devices.

On the other hand, internet downloads are the other method for the virus to get into the machine. Internet downloads is

the common activity that all computer users do. As a typical user we access the internet, do some activity, download application or program.

B. Spyware

A program that installed either with or without the user permission in order to collect personal computer information about users is a Spyware (DigiCert, 2022). Information regarding the users does not stop at personal information but they also do gather other information that is related to computer and browsing habits. According to Danial Javaheri, spyware collects all important and valuable data from the users (Danial Javaheri, 2018).

Figure 3 - Example of Spyware (Coustan, 2022)

A simple example of a spyware is shown in Figure 3. This spyware method is known as Browser add- ons. Out there in the internet world, there are thousands of activities similar to this. Almost every single user of the internet would have come across alerts similar to Figure 3.

There are few more other possible methods for the spyware to appear. Drive- by download is where there will be a pop up that installs the spyware. Nowadays, there are a number of websites that are developed with the spyware.

Piggybacked software installation is where the software that is being installed will be embedded with the spyware software. This usually takes place when free software is being downloaded and installed (Ankita Guha, 2020) .

Masquerading an anti-spyware is basically the spyware software that would pretend to be a tool to detect and remove the spyware. Mark B. Schmidt and Kirk P. Arnett has discovered that in 2005 the spyware have almost reached 90% of the users (Mark B. Schmidt, 2005). This indicates that, this spyware could take place at any time and the awareness of the spyware is crucial.

C. Worms

Malicious programs that develop copies of themselves repeatedly on any source such as local drive, network shares and more are known as worms. This worm does not harm any sort of data in the victims' machine.

On the other hand, the virus does bring a huge impact on the victim's machine. The worms basically would just take up the up spaces in the hard drive and they would also spread widely in the operating systems and the software used where it unveils all vulnerabilities in the victims machine.

W23. SillyFDC. BBY is one of the worms that is being developed and used on victims' machine (DigiCert, 2022). These worms are being sent to the victims' machine and these worms begin to generate copies of themselves repeatedly which will take up all the empty space in the machine and this will result on slowing down the machine and they tend to take up more network bandwidth. As they generate copies of themselves, they tend to spread into many programs causing them to disclose all the vulnerabilities that could be discovered in the victims' machine.

The worms are being picked most likely rather than the viruses (Saeed, 2020). The main reason for this selection is that the worms could be transferred from one machine to another one just with a network connection. Most of this attack takes place at location where there is free internet. The attackers will intercept the Wireless Access Point and spread the worm to those victims that connect to the free internet access.

D. Ransomware

Ransomware is a type of malware which has a behavior on taking control of the victims' machine (DANIAL JAVAHERI, 2018). This will later be used by the hackers to force the victims to pay either money or in cryptocurrency in order to provide the control back to the victims.

At one point the ransomware was so famous that it had become a topic of discussion. Ransomware was listed under the fourth phase of the malware evolution. The common method for the ransomware is by email, remote desktop, internet download and USB (Mohammed N. Alenezi, 2020).

At the current state, the ransomware is divided into two groups which is Encrypting ransomware and Locker ransomware (Nadeem Shah, 2017). Both of them have different purposes as the encrypting ransomware is where the encryption algorithms would block access to the files and locker ransomware is locking the operating system which will result on using the machine.

Srinivasan from Tata Communication has stated that, the ransomware variant Crypto Locker has infected almost more than 250,000 systems between September 2013 to December 2013 (CR, 2017).

The ransomware in 2013 had collected almost $3 million before they were taken down in 2014. In order to unlock those compromised files, an online tool was developed to recover them. This online tool was being used to recover the compromised files, but it has never been a solution to prevent the attacks.

Figure 4 shows an example lock screen that will display when the machine is being compromised to ransomware attack.

Figure 4 - CBT-Locker ransomware lock screen (TechTerms, 2022).

IV. Malicious Attacks on Industrial System

We have to understand that the attacks which are being conducted on an individual user would be much lower compared to attacks being done on industries. Industries are always the main prime victim for malware attacks. This is because, the industry stores millions of confidential information. When we hear the term confidential and one thing that comes to mind is secrecy. In 2020, almost all type of industries that provide different services had become a victim to malware attacks. Another reason to why industries are being the victim is because they are generating more income and they will have the capability to pay off millions in order to gain access back of their systems.

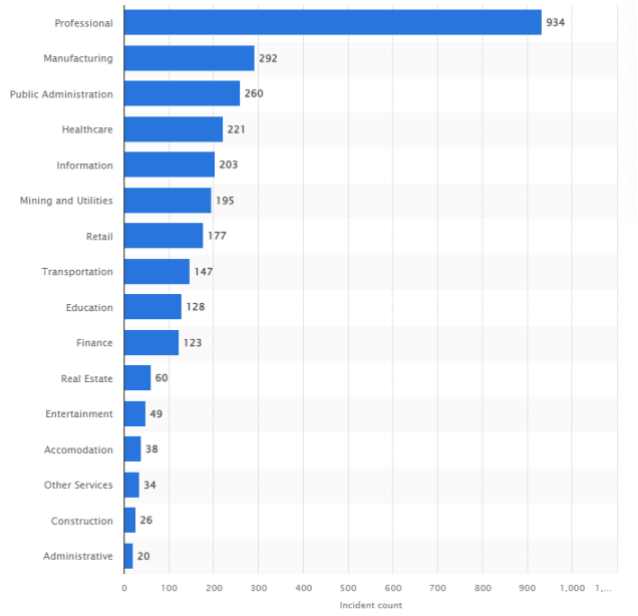
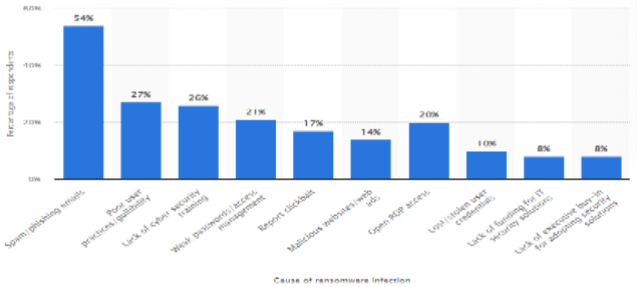


Figure 5. Global industry sector most targeted by malware incidents in 2020 (Johnson, Global industry sectors most targeted by malware incidents in 2020, 2022).

A clear display was given by Joseph Johnson in Figure 5. We can now be able to see the amount of malware attacks being conducted on industries. There were 934 malware attacks being conducted in the professional sector, 292 attacks in manufacturing, 260 attacks in public administrator and 221 attacks in healthcare. Almost all the industries that we can see in Figure 5 do carry a lot of confidential information. The one



attack that is being used on all those industries is ransomware and the method of the ransomware is different. There are different methods that the ransomware is being sent. Figure 6 shows, the methods used on causing ransomware. There are 10 different methods and each of them has their own ways.
Figure 6. Cause of ransomware infection (Johnson, Most common delivery methods and cybersecurity vulnerabilities causing ransomware infections according to MSPs worldwide as of 2020, 2021)

The spam or also known as phishing that is being conducted using the email has the highest occurrences as they are much easier to tackle or make the victim to voluntarily fall into the trap. This is because, when an email is sent and without a proper understanding and knowledge the victim would open the email to view. By viewing, the attack does not occur but if that email contains a clickable link or attachment and the victim did click the link or download the attachment then they would have gotten themselves into huge trouble. Industries do have thousands of employees and if the hackers send to every single employee the spam email, the hackers would just need to wait as there will have someone to click the link or download the attachment. This is where the ransomware begins after the hackers are in the victims' machine.

Back in 2014, roughly about 360 million accounts credentials and 1.25 million email addresses went up for sale in the dark web. This is a huge amount of information and that industries have become a victim. In order to overcome this the industries will have to pay the hackers in order for them not to sell in the dark web.

A. Malware and Cyberattacks targetting healthcare

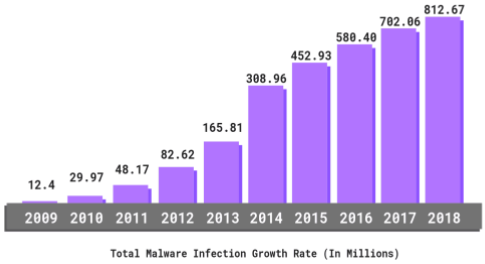
Healthcare is one the industries that stores plenty of confidential information compared to other industries (Watkins, 2014). This is because, they have more clients that are in the form of patients. Every single information of the patient will have to be stored. Information such as Name,

Age, Date of Birth (DOB), Identification Number, Disease, blood group and many more.

This information does carry a high value. Having that information being sold in the dark web could expose most of them and probably the patients could be victims for more illegal activities. In 2014, there was a survey that was conducted whereby the outcome showed the increase of cyber-attacks in healthcare and pharmaceutical areas would carry on.

Lately, the healthcare industry is facing pressure on how to improve patient care and controlling the cybersecurity attacks. Providing a high-class and proper patient care is one of the main goals for healthcare. On the other hand, protecting information regarding patients is a new norm whereby besides providing a proper patient care protecting patient information has its own level of importance. Failing on protecting that information would affect their business and they would face a huge drop on patient admission. This is the reason why hackers do pick healthcare as a victim.

The healthcare does have more confidential information compared to other industries. In 2020 alone, roughly almost 95 healthcare providers have become victims of malware



attacks and an estimated total of $15.6 million was paid for ransom (Shane Peden, 2021). This proves that healthcare will always be the number one victim when attacks takes place.
Figure 7 - Growth of malware infection (PurpleSec , 2022)

Figure 7 shows the growth of malware attacks. In 2014 a prediction was made that the malware attack on healthcare will increase and this proves that it was true. It will not stop here but in the coming years, the malware attacks will get more complicated, and the rates will increase drastically. This is because, as we are currently facing the Covid- 19 pandemic the hackers have begun to make use the Covid -19 scenario as a cover. Phishing emails are being used to conduct the ransomware attacks on victims. Figure 8 shows a simple example of the phishing attacks that is being distributed.

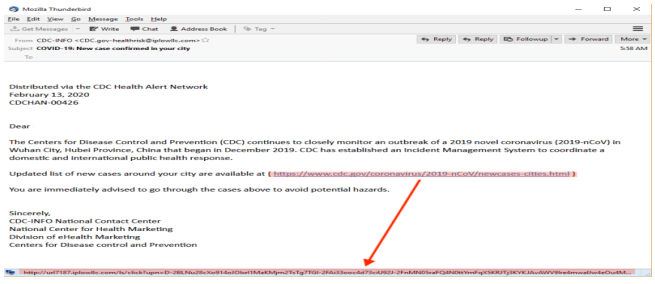


Figure 8 - Example of Phishing email (PurpleSec , 2022)

Basically, the email is simple and has straightforward content. The victim will just need to click the link that is provided to get an update on the list of new cases. Without knowing anything the user will click thinking it is a genuine link that provides that information. those links do open up a website that do contain that information, but those websites are not real they are developed by the hackers. Some emails will come with an attachment, probably the current statistics of the Covid-19 and those images would be developed with a backdoor for the hackers to conduct the ransomware when the user downloads the attachment.

Ransomware is one of the malware attacks. Healthcare do get two type of attacks which is Malware and Ransomware. They are being divided into two. The malware is the method being used for ransomware. Lauren E Branch has conducted research to learn the trend on malware attack and they have showed us a comparison of attacks that is done in USA Healthcare ntework. Figure 9, Shows the terminology used to describe the malware attacks. In Figure 9 we can see two terms being used which is malware and ransomware. This outcome result was made for the year 2016 and 2017. Comparing both years, the frequency or the rate of the attacks has increased. This small sample is enough to prove that in

Terminology	2016		2017		Total (N = 49)	
	Frequency	Percentage	Frequency	Percentage	Frequency	Percentage
Malware	5	22.73	3	11.11	8	16.33
Ransomware	17	77.27	24	88.89	41	83.67

upcoming years the rate of ransomware in healthcare is not going to decrease but they probably going to be doubled.
Figure 9 - Terminology used to describe attacks (Branch, 2019)

B. Why Healthcare?

Ever wonder why healthcare is being the most attacked industry? Looking from a technical angle, as industries are moving towards technology-based businesses, the process of business is going to be in alliance with the usage of technology. A simple example, in the earlier days the usage of paper is more frequent but with the current adoption rate the usage of paper is down as nowadays that information on the paper is being converted into softcopy files and stored in the cloud with a server to access. This would provide an example on how businesses are moving towards technology adoption. Beyond these upgrading there are a number of issues that makes the healthcare to be a sector to be attacked (Malcolm Harkins, 2018).

I. Lack of preparation

Preparation is a factor that is needed to be taken into consideration before doing any tasks. As we believe, industries are starting to adopt the technology, and this will indicate that the industries are not fully prepared if an attack takes place. This is because, as the development of technology takes place the precaution of the attacks will take some time as they will only be able to work on the precaution as when attacks happen. Healthcare has been practicing the

traditional method of using hardcopy documents and when they begin to adopt the technology, they tend to take a longer time to adapt and move the business into the technology approach. This would prove that there will be a lack of preparation as they are all new to this norm. Cybersecurity is not given the full priority as the industry does not want to invest on it until and when an attack has taken place. This would give the indication on the lack of preparation and the hacker would take is as an advantage to them.

II. Lack of security awareness

Awareness on cybersecurity and its dark side plays a vital role on educating and preventing any attacks. Awareness will need to be given on all aspects as this will give a brief idea or knowledge on what is happening. Employees will be able to take precautions via safe steps and it could prevent them from falling into the traps that is being set by the hackers. Without the proper awareness the employees could be the victim to all sort of malware attacks. For instance, email phishing without the awareness of it could be a huge easy method for healthcare. With sufficient awareness and training these methods could easily be eliminated.

C. Classification of attacks on Healhcare

Type of Attack	Description	Output
Email Phishing	Email attachment and Uniform Recourse Locators (URLs)	Ransomware
Remote Desktop Protocol	Work from home remotely	Ransomware
Exploits Kits	Website that has Malicious code	Ransomware
Watering Hole Attacks	Website changed	Ransomware
Removable Media Universal Series Bus	Physical entrance	Ransomware
Installing Private Software	Downloading software application	Ransomware
Microsoft Office Macros	Microsoft Office (MS) office macros suffer from malicious activities	Ransomware

Table 1 - Malware attacks method on healthcare (Noor Thamer, 2021)

Table 1 shows a list of malware attacks that is conducted on Healthcare. As we know there are plenty of malware attacks and the malware attacks methodology is listed in Table 1. A brief discussion will be given below which will give a clarification on the types of attack.

a. Email Phishing

Ever wonder why we sometimes receive emails from some unknown sender? Ever wonder why are there clickable links or an attached image? Email phishing is one of the methods whereby the hackers would create an email that looks genuine. Those emails either contain an attached image, document, or a Uniform Recourse Locator (URLs) that would open up a website (Akarshita Shankar, 2019). Social engineering is being included in the attachment or the URLs (Zainab Alkhalil, 2021). Upon downloading or clicking the links, a script or executable file would begin to execute worms and virus which will provide further information for the hacker on the vulnerability in the computer system. With that information the hackers could lock all files, and this will slowly be changed into ransomware. For instance, in 2014 a cybercriminal sent an email phishing to Premera Blue across all of the healthcare's employees (Bernstein, 2019). That email was implanted with an attached document that consist of social engineering. When the employee clicked on it the cybercriminal had his opportunity to get into the healthcare's server. The healthcare had to pay off $74 million as a settlement.

b. Remote Desktop Protocol

As we are living in the Covid-19 pandemic, work for home has become a new norm for all industries. This is mainly to prevent the spread of the Covid-19. By having work from home (WFH), this has helped many companies on cutting down cost and this allowed them to shut down a number of facilities. This allows them to cut cost and gave more flexibility for the employees. But the hackers took this as an opportunity to conduct their attack on company servers through the employees. The work from home model allowed for remote access to be provided for the employee to access the company server. For instance, a hacker has the ability to attack the employee of the particular healthcare company and later they would conduct a brute force or even keylogger which will allow the hacker to retrieve the username and credentials of the sever access (ZiHan Wang, 2018). Once the hackers are able to access the server then they will begin the ransomware by encrypting those files in the server.

c. Exploit Kit & Watering hole attacks

Almost in all websites a user access would come with an advertisement. Have you ever wondered if those were genuine advertisements? Not all advertisements are genuine. Out there, there are hackers who have used exploit kits to develop an advertisement that's gone through social engineering to link the advertisement with a malicious code (Ade Kurniawan, 2017). This malicious code will be executed when the user clicks or open them.

Watering hole is an act that could be related to the exploit kit as watering hole is defined as an act of injecting malicious scripts into Hypertext Markup Language (HTML). The hackers will begin to view which website the user does access frequently and then they will begin to inject the malicious scripts into the website and when the user accesses the website (Ms. V. Revathi, 2018). With the exploit kit and

watering hole attacks, the hackers will be able to access the user's computer and later they can implement the locker ransomware and demand a ransom to unlock it.

d. Removable Media Universal Series Bus

This type of attack is done with a low rate as this action requires a physical action. The hackers will need to physically insert a removable media such as USB, Hard Disk and more. This is riskier as they need to get physically to the user's computer and insert the USB in order for the malware to spread into the user's computer. In 2020, a report showed 30% of the attacks were done with a USB (Nagel, 2021). This proves that they are riskier and thus they do have a low percentage but still the hackers do tend to take risks.

e. Private Software

The term private software is used more frequently on huge organizations. This is because, private software is not a safe action as most of the time they are intact with malicious codes which will begin to attack the computer when they are installed. This is only reason organizations do not support private software as this will allow the hackers to access into the computer and later attack the organization server and begin the ransomware.

f. Microsoft Office Macros

This method of attack is usually being combined with other methods. Basically, what happens here is that the cybercriminal will probably conduct a man in the middle attack, whereby they will attack the network and begin to capture the connection between two employee system conversations. Instead of network connecting both computer it will now loop them to a third computer without their knowledge. This will allow the cybercriminal to view what is being shared between them. They will also have the chance to amend the item and send pass it. This is an opportunity for the cybercriminal to attach the malicious macro in the Microsoft document and release it to the receiver (Zurkus, 2018). Thinking that it is coming from the colleague, the employee will download and open it. Without them knowing the malicious code that is inserted in it, the macros will execute and then the Locky ransomware is applied.

D. Real Case Cyber Attacks on Healthcare Industry

1) Case 1: Sing Health

Sing Health is a Singapore based Healthcare provider. In the year 2018, they faced a huge attack on their server. There was a data breach on personal information of 1.5 million patients (Davis, 2019). The prime minister Lee Hsien Loong's personal information was one of it that was extracted during the data breach. The main reason for the data breach to take place is a bad system management. Besides that, poor employee training and flaws on the system are also reasons for the breach to take place.

Once the breach took place, a committee was formed to investigate work on a solution. A discovery was made whereby, the attack or also known as the data breach was running since 2017 and it was estimated to be happening almost a year from 2017 to 2018. The data breach also included 160,000 medical data of patients.

The committee also reviewed and discovered that there were poor employee awareness trainings. This was an issue which allowed the data breach to take place. This is because, when the employee does not have enough training or awareness, they would not have enough knowledge to know what is happening. Probably the attacks would be conducted with the presence of the employee and if there is brute force being taken and error or notification being popped up the employee would not know about it, and they might just oversee it.

Beside poor training there also did find out there are plenty of flaws in the network. These flaws have become a pathway for the data breach to take place. It is said, there was an indication that there were suspicious login attempts being made into the Sing Health's database. Those attempts were recorded but they failed to categorize the attempts as a threat. Failing to categorize the attempts was a flaw and this helped the attacker to conduct the attack for a year without being noticed.

Coding vulnerability is the method the attackers used on accessing the database. These coding vulnerability actions were used in the network connection that provide sconnection between the Citrix servers at the public hospital and their database. The Citrix serve was not secured with unauthorized access, and this allowed the attacker to penetrate them. A pen test was conducted on the server and there were a number of vulnerabilities that have been raised but the action was limited.

Therefore, the presence of data breach on the Sing Health was mainly due to human mistakes. If there were proper action taken for the vulnerability that they discover during the pen test, then this data breach would not happen. Training session should also be given for the employee on the cyber-attacks and how to react to them.

2) Case 2: Universal Healthcare Service

Universal Healthcare Service is a hospital and also a health care network that has more than 400 facilities (O'Donnel, 2021). Somewhere in 2019 Universal Healthcare Service faced an attack which brought them to face a number of issues. Due to the breach the cost included loss of revenue, ambulances were diverted to different hospitals, bills were delayed and many more for more than two months. This is because, the breach was not only for data but for ransom as well.

This ransomware had delayed so many processes and even smaller clinics were instructed to close as they were not able to access patients' records. Having this sort of issues would most likely bring down the image of the healthcare provider and data of patients could be sold in the dark web.

V. CONCLUSION

In summary, malware has always been there. Cybercriminals will always wait for an opening. With proper cybersecurity,

training, and knowledge for the employee, cyberattacks could be eliminated easily. Flaws on server, network and systems would be more useful for the cybercriminal as this is a vulnerability and the cybercriminal would use these vulnerabilities to attack.

Lately during the Covid-19 pandemic era, healthcare has become a target for malware attacks. These attacks are made via different methods, but the output would be the same which is ransomware. Upon getting the virus, worm, and other sort of malware then the cybercriminal will either encrypt files or the lock the computer and demand a ransom amount in order for them to unlock their actions.

REFERENCES

1. A. K. Maurya, N. K. (2018). Ransomware: Evolution, Target and Safety Measures. *International Journal of Computer Sciences and Engineering*, *6*(1), 80-85.
2. Ade Kurniawan, A. F. (2017). What is Exploit Kit and How Does it Work? *International Conference on Innovative Research in Science, Technology and Management*, 1.
3. Akarshita Shankar, R. S. (2019). A Review on Phishing Attacks. *International Journal of Applied Engineering Research* , 2171-2175.
4. Ankita Guha, A. M. (2020). Role of Spy-ware Analysis in the Arena of Cybersecurity. *International Journal of Scientific Research in Computr Science, Engineering and Information Technology*, *6*(6), 268-273.
5. Bernstein, M. (30 July, 2019). *Premera Blue Cross to Pay $74M Over Data Breach*. Retrieved from Goverment technology: https://www.govtech.com/security/premera-blue-cross-to-pay-74m-over-data-breach.html
6. Branch, L. E. (2019). Trends in Malware Attacks against United States Healthcare Organizations, 2016-2017. *Global biosecurity*.
7. Coustan, D. (2022). *How Spyware Works*. Retrieved 14 February, 2022, from https://computer.howstuffworks.com/spyware.htm
8. CR, S. (2017). *Hobby hackers to billion-dollar industry: the evolution of ransomware*. Retrieved 21 February, 2022, from https://isiarticles.com/bundles/Article/pre/pdf/145709.pdf
9. Danial Javaheri, M. H. (2018). Detection and Elimination of Spyware and Ransomware by Intercepting Kernel-Level System Routines. *Digital Object Identifier*, *6*(1), 78321- 78332.
10. DANIAL JAVAHERI, M. H. (2018). Detection and Elimination of Spyware and Ransomware by Intercepting Kernel-Level System Routines. *IEEE*, *6*(1), 78321-78332.
11. Davis, J. (10 January, 2019). *Massive SingHealth Data Breach Caused by Lack of Basic Security*. Retrieved from Health IT Security: https://healthitsecurity.com/news/massive-singhealth-data-breach-caused-by-lack-of-basic-security
12. DigiCert. (2022). *What are Malware, Viruses, Spyware, and Cookies?* Retrieved 14 February, 2022, from https://www.websecurity.digicert.com/security-topics/what-are-malware-viruses-spyware-and-cookies-and-what-differentiates-them
13. Forcepoint. (2022). *What is Malware?* Retrieved 11 January, 2022, from https://www.forcepoint.com/cyber-edu/malware#:~:text=Malware%20is%20the%20collective%20name,unauthorized%20access%20to%20a%20network.
14. Johnson, J. (16 February, 2021). *Most common delivery methods and cybersecurity vulnerabilities causing ransomware infections according to MSPs worldwide as of 2020*. Retrieved from Statista: https://www.statista.com/statistics/700965/leading-cause-of-ransomware-infection/
15. Johnson, J. (2022). *Global industry sectors most targeted by malware incidents in 2020*. Retrieved 24 February, 2022, from https://www.statista.com/statistics/223517/malware-infection-weekly-industries/
16. Vinesh Thiruchelvam (2020), “Malaysian Online Behaviour and Practices – A Survey Study Output”, International Journal of Management (IJM) Volume 11, Issue 10, October 2020, pp. 1824-1830. Article ID: IJM_11_10_170
17. Landesman, M. (09 March, 2021). *A Brief History of Malware.* Retrieved 11 February, 2022, from https://www.lifewire.com/brief-history-of-malware-153616
18. Malcolm Harkins, A. M. (2018). The Ransomware Assault on the Healthcare Sector. *: Journal of Law & Cyber Warfare*, 148-164.
19. Mark B. Schmidt, K. P. (2005). Spyware: A little knowledge is a wonderful thing. *Communication of the Acm*, *48*(8), 67-70.
20. Milind J. Joshi, B. v. (2013). Computer Virus: Their Problems & Major attacks in Real Life . *International Journal of P2P Network Trends and Technology (IJPTT)* , *3*(4), 206-209.
21. Vinesh Thiruchelvam (2020), “Recent Cyber Breaches in Malaysia and Possible Countermeasures”, International Journal of Solid

State Technologies Volume 63, Issue 6, December 2020, pp. 17478-17487.

22. Mohammed N. Alenezi, H. A. (2020). Evolution of Malware Threats and Evolution of Malware Threats and. *International Journal of Communication Networks and Information Security (IJCNIS), 12*(3), 326 - 337.

23. Ms. V. Revathi, R. P. (2018). An Overview: Watering Hole Attack . *International Journal for Scientific Research & Development*, 2011-2013.

24. Nadeem Shah, M. F. (2017). Ransomware - Threats, Vulnerabilities And Recommendations . *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY, 6*(6), 307-309.

25. Nagel, D. (22 June, 2021). *Malware via Removable Devices Nearly Doubles*. Retrieved from THE Journal: https://thejournal.com/articles/2021/06/22/malware-via-removable-devices-nearly-doubles.aspx

26. Noor Thamer, R. A. (2021). A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research. *International Conference on Information Technology and Science* , 210-216.

27. O'Donnel, L. (02 March, 2021). *Post-Cyberattack, Universal Health Services Faces $67M in Losses*. Retrieved from threat post: https://threatpost.com/post-cyberattack-universal-health-services-faces-67m-in-losses/164424/

28. Omoth, T. (2021). *How computer viruses spread and how to avoid them*. Retrieved 21 February, 2022, from https://www.itpro.com/security/malware/357313/how-do-computer-viruses-spread

29. Vinesh Thiruchelvam (2019), 'Cyber Treat', Journal of Advanced Research in Dynamical and Control Systems', Volume 10, Issue 11, Feb 2019, Pg228-231

30. Radware. (2022). *The History of Malware*. Retrieved 14 February, 2022, from https://www.radware.com/resources/malware_timeline.aspx/

31. Saeed, M. A. (2020). Malware in Computer Systems: Problems and Solutions. *International Journal on Informatics for Development, 9*(1), 2-8.

32. Shane Peden, M. R. (09 June, 2021). *Clinical treatment of ransomware in healthcare*. Retrieved from Security: https://www.securitymagazine.com/articles/95381-clinical-treatment-of-ransomware-in-healthcare

33. TechTerms. (2022). *Ransomware*. Retrieved 21 February, 2022, from https://techterms.com/definition/ransomware

34. Vijayanand, A. (2019). Impact of Malware in Modern Society. *International Journal of Scientific Research and Engineering Development, 2*(3), 593-600.

35. Watkins, B. (2014). The Impact of Cyber Attacks on the Private Sector. *Association for International*, 1-11.

36. Webroot Inc. (2022). *What is a Computer Virus and How Can I Protect My Computer?* Retrieved 21 February, 2022, from https://www.webroot.com/us/en/resources/tips-articles/computer-security-threats-computer-viruses#:~:text=Examples%20of%20computer%20viruses&text=Trojans%20%2D%20As%20in%20the%20myth,a%20ransom%20for%20its%20return.

37. Zainab Alkhalil, C. H. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, 1.

38. ZiHan Wang, C. L. (2018). Automatically Traceback RDP-Based TargetedRansomware Attacks. *Wireless Communications and Mobile Computing*, 13.

39. Zurkus, K. (14 September, 2018). *Microsoft Office Macros Still No. 1 Malware Delivery*. Retrieved from Info Security: https://www.infosecurity-magazine.com/news/microsoft-office-macros-still-no-1/