International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-2, December, 2019

Four Most Famous Cyber Attacks for Financial Gains

Asalah F Altwairqi, Mohammed A. AlZain, Ben Soh*, Mehedi Masud, Jehad Al-Amri

Abstract: ***Cyber attacks are on the rise every day and pose a major threat to the Internet users. Cyber attackers are constantly capable of gaining hidden exposure at the moment and keeping a low profile. There is a need to carry out analyses on cyber attacks for educational purposes. In this paper we analyze four types of most famous cyber-attacks for financial gains: phishing attack, salami slice attack, ransomware attack, and cryptojacking attack. General Terms: Cyber attacks***

Keywords: ***Phishing, salami slicing, ransomware, cryptojacking.***

I. INTRODUCTION

The use of the digital world has increased rapidly worldwide. All the tedious day-to-day operations are made easier, faster and safer through the Internet. For example, you can shop at home, you can apply for a job at home and you can transfer and do all the financial operations at home. Unfortunately, the Internet is a double-edged weapon. In other words, it may contain good people and evil people.

The most important question here is how to take advantage of the services provided by the Internet without putting personal information at risk [1] [2] [3] [4]. To do this we should be aware of the problems (attacks) that we may have and know how to deal with them.

This paper focuses on some of the attacks that are intended to make money. We will analyze the four most famous attacks, namely phishing attack, salami slicing attack, ransomware attack, and cryptojacking attack.

First, the phishing attack is to deceive the user for sensitive information, whether personal or financial, and often stolen information is used to transfer money illegally[5]. Second, the salami slicing attack is theft of small quantities, whether information or money, without the realization of the user[6]. Third, the ransomware attack is locking your computer or blocking access to information by malicious software until the ransom is paid [7]. And finally, the cryptojacking attack is mining of cryptocurrency (bitcoin, Ethereum. etc.) by hijacking a user's web browser[8].

Revised Manuscript Received on December 30, 2019.
* Correspondence Author
Asalah F Altwairqi, College of Computers and Information Technology, Taif University, Saudi Arabia
Mohammed A. AlZain, College of Computers and Information Technology, Taif University, Saudi Arabia
Ben Soh*, La Trobe University, Bundoora 3086, Australia
Mehedi Masud, College of Computers and Information Technology, Taif University, Saudi Arabia
Jehad Al-Amri, College of Computers and Information Technology, Taif University, Saudi Arabia

This paper is organized in the following format. Section II discusses the methodology of this research. Section III describes the origin of the four cyber attacks mentioned above. Section IV focuses on the various types of the four cyber attacks in detail. Section V explains the tools and techniques used to initiate an attack. Section VI describes how they work. Section VII presents the losses due to the attacks. Section VIII discusses how to protect yourself from these attacks. Section IX briefly presents the timeline of the attacks. Section X shows the general statistics of the cyber attacks as of 2019. Section XI provides the result. Section XII concludes the paper.

II. THE METHODOLOGY

The paper analyzes four cyber attacks for financial gains on the qualitative point of view. The data used in the paper was collected from other scientific research in addition to reports submitted from antivirus programs. The research methodology is depicted in the following Figure 1.

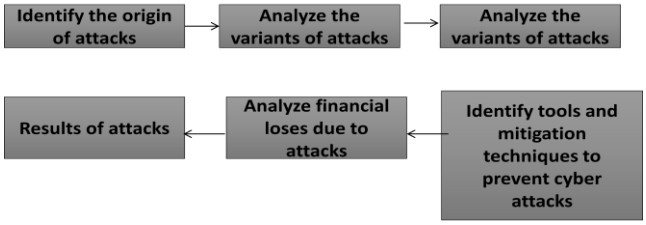

Fig 1 : Methodology of research

III. THE ORIGIN OF THE ATTACKS

The history of the attacks is dated back to the 1980s. But with the spread of the Internet, the attacks have become more widespread and well known.

A. Phishing attack

Phishing started on the America Online (AOL) network systems in the early 1990s. Some hackers created fake accounts using a fake credit card number and ID. Despite the incompatibility with the actual cards and the owner identities, the accounts still passed simple validation tests performed by AOL because of a weakness in the system. As a result, AOL believed that the accounts were legitimate. The fake accounts remained active until they were billed and found to be invalid [9].

The creation of counterfeit accounts is not in itself a phishing process, but it was the beginning of developing the phishing process [9].

By the mid-1990s, AOL have immediately verified credit card numbers and associated identities. This had changed the ways how the hackers got AOL accounts. Instead of creating new accounts, fraudsters steal legitimate accounts for other users. In order to do this, fraudsters communicate with legitimate users and persuade them to reveal their information such as a password in the pretext for security purposes as employees [9].

B. Salami slicing attack

Salami slicing is based on the old "collect-the-round off" trick. The attacker utilizes mathematical routines such as value calculations. The calculations are done based on decimal places, usually 2 or 3 places. For example: If we had a dollar currency, we will be rounding to nearest penny then forgetting the rest of the decimals. The attacker can transfer these fractions of pennies to his account with no warning to the financial institution [6].

C. Ransomware attack

The first virus of ransomware was created by Joseph L. Poppt in 1989. He distributed the virus by floppy disk at the World Health Organization's International Aids conference. The malicious software will count the number of times the computer was booted and once it reaches 90 it encrypts [10] [11] or lock the file names. To restore access, users will have to send $ 189 to PC Cyborg Corporation in a mailbox. It was very easy to break because it uses simple symmetric encryption. It is called the AIDS Trojan (and also known as the PC Cyborg)[7].

D. Cryptojacking attack

The first appearance of cryptojacking was in 2017 when the Coinhive website published code that enabled cryptominers to extract cryptocurrency. After that, the peer-to-peer file-sharing Pirate Bay site incorporated this code into their website, inviting its customers to use this method to generate money for Pirate Bay. After Coinhive appeared, malicious counterfeit websites emerged online to provide similar scripts that enabled miners to illegally seize computing resources for mobile devices, personal computers, and servers[12].

IV. VARIANTS OF THE ATTACKS

Depending on the technological development, the attacks will also develop their methods and gain all possible opportunities to create an attack. To do this, each attack branched into several types.

A. Phishing attack

Although the attacker' final goal is always the same, they have found various ways to launch their attack. Here are some of the most common ways in which they target people.

- Spear phishing: It is one of the most popular strategies which accounts for 91% of attacks. This is done by using the victim's personal information to gain trust, thus increasing the likelihood of success[13].
- Whaling: It mainly focuses on senior managers of an organization. Sometimes, email material is published as a legal subpoena, client grievance, or executive issue. This suggests there is some kind of company-wide falsification [14].
- Clone phishing: It is another form of traditional phishing attack in which a genuine email is duplicated to replace the attached files in the email or direct the user to an entirely fake form... [14].

The above phishing types are traditional because they rely on emails. Emails are a service done through network. But there are still many services that can be exploited. So the attackers developed some other methods, as follows.

Smishing

The word SMiShing derived its name from the SMS (Short Message Service) text messaging technology. It is a type of phishing using SMS or text messages on mobile phones or smartphones. There are two main SMiShing scams processes[15]:

The first main scam occurs when a trusted source such as a bank or system administrator sends a text message.

The second main scam occurs when a victim receives a text message with sensitive content, such as an account freeze or a stolen identity. The victim is then directed to a fake website or phone number to verify the information.

Vishing

The word "Vishing" is derived from a combination of "voice" and "phishing". It is said to be done when the attacker communicates with the victim to provide sensitive information such as financial or personal information for financial purposes through technology based on IP voice messaging[16]. With sensitive victim's information, the attacker gains the victim's confidence easily. This is because the victim believes it is difficult to falsify the caller ID or other phone services.[17].

B. Salami slicing attack

Salami attack is divided into two types [18, 19]:

- Internal attacks: They are the most widespread. The attacker is very familiar with the security system. For example, a bank employee inserts malicious software into the bank's server that will divert one SR from each customer that makes a transaction from his work station to his account.
- External attacks: They happen outside the organization. When an attacker leaves the organization with the knowledge of the security system, he/she tries to steal information that causes serious damage to the organization.

C. Ransomware attack

There are two major types of ransomware. The most popular one is crypto ransomware that encrypts computer data and files. The other type is locker ransomware that executes a lock-down of the victim computers, software or other devices like mouse and keyboard.

- **Crypto ransomware**

It is a file and data malware that runs silently searching for user data and files after being injected into end user systems. However, the systems that are infected continue to function normally because the important files of OS and files of applications are not targeted,

So the functionality of the victim system is not affected. After that the malicious software encrypts data and files from the victim that make data and files useless for the victim and request an amount of money (ransom). This enforces the victim to pay for the decryption key. Crypto ransomware is designed to scan for end-user or extension files such as FLV, PDF, RTF, MP3, MP4, PPT, CPP, ASM, CHM, TXT, DOC, XLS, JPG, CGI, KEY, MDB and PGP[20].

- **Locker ransomware**

It affects hardware, such as end-user computer systems and mobile devices, or equipment such as mouse and keyboard control interfaces, by locking them or denying access to the device user. The ransomware displays on the computer screen and provides limited access to some required functions such as keeping the numeric keyboard keys and moving the mouse that allow the victim to enter, after that the victim needs to pay the required ransom to get back the full access [20].

D. Cryptojacking attack

As mentioned earlier, this type of attacks appeared in 2017 so it still new and did not branch into other species. It is a science in itself. There is no need for branching.

V. TOOLS AND TECHNIQUES USED IN THE CYBER-ATTACKS

Before knowing how attacks work in particular, you should know the techniques that the attacker generally uses to initiate an attack.

A. Port scanning

Port Scanning is a technique used by hackers or crackers to identify the active port or port being used over the network. By using different hacking tools, a hacker can send data to UDP or TCP over the ports at a time. From these ports, a response is generated that the hacker receives and can determine whether or not the port is in use. The hacker can also focus on attacking ports that are open with the received response and then try to gain access by exploiting any weaknesses[21].

B. Cracking of password

All system cache passwords in the memory during the login session. The hacker may therefore try to gain access to the system's memory to sift the memory in order to access the stored passwords. The hacker can frequently perform this task by sifting password files. Cracking a password requires to decrypt it or bypass its protection scheme. Another way to crack a password is to combine letters, symbols or numbers to create all possible combinations of a password and then try to find the right password one by one[21].

C. Sniffing of packets

Packet sniffing is capturing the data packets that flow across the computer network by using a packet sniffer which is a specific device or software used to perform this task. Also, it can monitor network performance or to solve any network problem[21].

D. Key controller

A key controller is a device or software that can monitor and record key presses on a computer system's keyboard and thus all user-typed keys can be viewed by installing this device or software. Therefore, by getting access to all the user-typed keys, any hacker can get the user-typed data and device passwords that they don't want others to know about[21].

VI. MODUS OPERANDI OF THE ATTACKS

Attacks are a battle between the attacker and the user. To win the battle the first line of defense is to know how the attacker works.

A. Phishing attack

A phishing attack consists of three main steps[9]

- The lure: Attacker tries to persuade the victim to click on a link to open a fake website or download a malicious program (without knowing the victim).
- The hook: The victim is trapped, for example, opening the link sent by the bank and entering the information.
- The catch: It is theft and use of information, for example, the transfer of funds from the victim's account to the attacker's account.

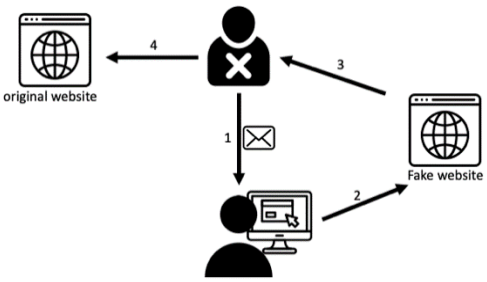

Fig 2 : Phishing attack

In the first step, the attacker sends an e-mail to the victim containing a link to a fake website similar to the original site. When the victim opens the fake site and enters the required information such as password and username, the information is sent to the attacker (Steps 2 and 3). Surely the attacker will be able to use the password and username in the original site and this is what Step 4 shows.

B. Salami slicing attack

The attackers steal resources or money a little at a time in the salami technique. The important thing here is to make the change meaningless and no one will notice it completely. For example, an employee of bank installs a software into the servers of the bank, which takes a small amount of money from each customer's account. Every account holder isn't likely to notice this illegal deduction, but every month the attacker will make a substantial amount of money.

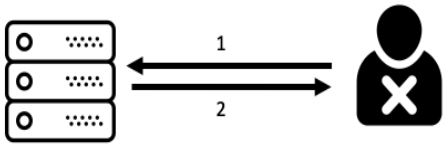

Fig 3 : Salami attack

The attacker installs malware on the server so that it performs a specific purpose, such as installing malware on the bank' server and its purpose is to deduct small values of money and send it to the attacker without giving an alert.

C. Ransomware attack

Similar to the way phishing attack works. The attacker first persuades the victim to click on a link or download a program. Once the victim falls into the trap, the attacker locks the computer or blocks access to the data. The attacker requests a sum of money (ransom) to deactivate the malicious program[7, 22].

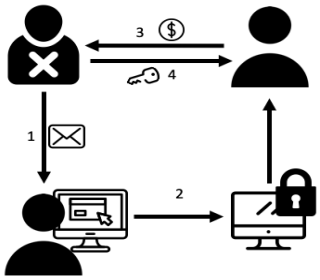

Fig 4 : Rrensomeare attack

The attacker sends e-mail containing malicious files that lock some computer services or the entire computer or encrypt data[23] [11] (Steps 1 and 2). The victim must pay the ransom to the attacker and in return will receive the key to decrypt[24] or restore services (Steps 3 and 4).

D. Cryptojacking attack

There are two methods to launch an attack:[12, 25]

- **Malware scripts**

Here the user downloads a malware-containing link that downloads code installed on your computer to start cryptocurrency mining from it. This type of attacks obtains your computer resources that is cryptojacking generally does not harm your computer, unlike traditional malware. But of course, there are exceptions, for example, Loapi is an Android malware that is so aggressive in cryptojacking that it will actually harm your device.

- **JavaScript code in browser**

Through inserting malicious JavaScript code into a web page, the hacker attacks several devices. Any device can become cryptojacked when the victim browses an injected page. However, not all in-browser cryptocurrency mining approaches are malicious.

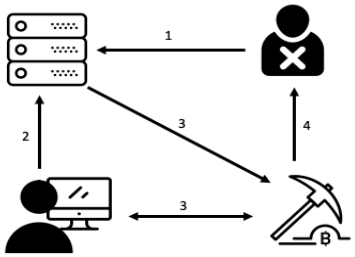

Fig 5 : Cryptojacking attack

The attacker and the victim are both connected to the server where the attacker uses one of the previous techniques to control the user's device (Steps 1 and 2). This allows the attacker to explore and send coins (Steps 3 and 4).

VII. LOSSES DUE TO THE ATTACKS

One of the most famous and major **phishing** attacks is **Phish Phry** in 2009. It is an operation in which attackers targeted hundreds or even thousands of accounts in US banks. They stole their information and used it to transfer money into fake accounts under their control. The attackers stole US$ 1.5 million[26, 27].

Muller (the sixth Director of FBI, 2001 - 2013) made the remarks during the National Cyber Security Awareness Month; "Cybercrime might not seem real until it hits you," Mueller said. "But every personal, academic, corporate, and government network plays a role in national security"[26]. This shows the importance of protecting ourselves and our society from attacks.

Another example of one of the biggest attacks carried out is **WannaCry Ransomware** attack in 2017. It locks all the user data on a computer by writing the encrypted contents in-place after opening and reading the file, then closing the file. It leaves only two files to instruct the user about what user should do next and how to decrypt program. Hackers demand payment in bitcoin, otherwise giving warning that the files will be deleted [28].

The two previous examples are phishing and ransomware. Although it was only two attacks on different dates, the damage it caused was very large. Sometimes damage extends to years like Yahoo, Panic at Sony, and Adobe that was going through hell. These examples are immortalized in history because of the great damage they have caused.

VIII. MITIGATION TECHNIQUES AGAINST THE ATTACKS

Knowing the techniques used and the mechanisms of an attack is the first line of defense. But is it enough? Unfortunately, it is not. We also need techniques and tools to help prevent attacks and certainly we cannot prevent all attacks so we have to detect them.

A. Phishing attack

There are many techniques used to detect and prevent phishing attack. It is possible to use more than one technique at the same time. We cannot prevent email spoofing from targeting the victim, but the victim can be smart and win this battle by:

- **Using spoofed email detection**

That is to identify spoofed address by setting your junk filtering. Do not trust the email's display name because most hackers use the organization's name. Just "anchor text" is shown in the web browser in this form of email, but not URL. To solve these problems, the Link Guard algorithm [29] is used. Phishing email connection characteristics build an algorithm with a set of policies like discovering hyperlinks with the actual link distance[30].

- **Using fake social networking accounts detection**

Social networking sites need to follow laws to prevent the production of fake profiles[31-34], but there is a lack of proper enforcement to identify the user[35].

The intruder makes fake account to exploit someone's trust.

Table 1: Phishing, ransomware and cryptojacking attacks stats for three years

Year	Pishing	Ransomware	Cryptojacking
2017	91	11	13
2018	236	7	6
2019	240	14	7.7

Typically, the user shares their personal information in their profile and status. In order to prevent this type of attack, the user should be constantly aware of what they post, what they upload, and the user should be particularly aware of the media they share with others when using links[30].

- **Using hacking detection**

Here, you need to use antivirus software. Antivirus software is crucial in maintaining a good and stable computer. And you need to download from a trusted website with updated programs, software and anti-viruses.
You should be mindful of this while using the Internet; when you click on a link to fraud, your email may be compromised. The security of your password should be high that the hacker can't easily guess. Keeping your banking and other financial accounts password secure and secret is particularly important. The password should be 3D: numbers, alphabet, and special character can be used[30].

- **Using Trojan horse detection**

When uploading a file from the Internet, you have to be alert. Being a victim of a Trojan horse is only a matter of time since it deludes you as a useful program.
Always remember that you can't trust anyone even your friends. Always check the content of the file sent to you before opening or running. Because Trojans publish themselves in files, in programs or even in email address book in the friend list.
You should take care of the extension of the file, because some operating systems like Windows hide by default the last extension of a file. For example, "Susie.jpg" could look like "Susie.jpg.exe,", which is a Trojan executable [30].
No single technology will prevent phishing absolutely. A combination of good organization and training, the proper use of current technologies and developments in security technology, has the potential to drastically reduce the incidence of phishing and its losses [36].

B. Salami slicing attack

To prevent this attack, we need every possible protection technique. Because we do not know where the attacker was from, be it within the company or from outside. These are some of the techniques required[37] :

- **Physical security**

Physical security is the most important aspect of cybercrime prevention. Where computer network should be protected from unauthorized people's access.

- **Access control system**

Access is often controlled by a firewall that provides a central point through which access is allowed and disallowed. Firewalls allow only authorized network communications, be it internal or external.

- **Password**

Proving the identity is a necessary element for the detection of an attacker. Identity verification is done using a password system and is the most common method used by servers, routers, and firewalls. Most of the programs were designed to ask for username and password for computer system entry. This gives the client assurance. Password should be 3D: numbers, alphabet, and special character can be used.

- **Finding The security holes in networks**

Before the intruders do, system security administrators must monitor the gaps. Most network suppliers do not have sufficient knowledge of the security holes' details. Organization should therefore work hard to discover holes, bugs and weaknesses in security and report their findings as confirmed; especially if they contain sensitive information such as banks.

- **Using network scanning programs**

They are available as a free tool on the Internet. It aims to administer the security. This application searches and collects information about any host on a network, regardless of the operating system or services run by the hosts. It monitors the vulnerabilities as glitches, security flaws, insufficient password protection, etc. COPS (Computer Oracle and Password System) is another product available. According to CERT safety alert times, it checks for weak passwords, hazardous folder access, and main file dates.

- **Using intrusion alert programs**

An example is using intrusion systems detecting suspicious activity and monitoring in order to take necessary action. It should act continuously so that all suspicious network activity is quickly captured.

- **Using encryption**

The ability to transform information into a form that makes reading without the right key is almost impossible. The key is used to allow selected people to have managed access to the information[38]. Anyone can have the information, but the data can only be accessed by people with the right password. Encryption enables private documents to be sent by e-mail or private information to be stored on computers without fearing that the data will become public if someone steals it[39].

C. Ransomware attack

Popular techniques used to prevent this attack include:[40]

- **Machine learning**

It involves learning the patterns of creating a model in data. Once fed with new data, this model can then predict the outcome[41]. However, the most difficult thing about using ML is to find the appropriate algorithm to match the data type and the required result.

Table 2 : Comparison between phishing , salami slicing , ransomware and cryptojacking attacks

	Phishing attack	Salami slicing attack	Ransomware attack	Cryptojacking attack
Year of appearance	1990	1993	1989	2017
Types of attacks	• Traditional phishing: Spear phishing, Whaling and Clone phishing • Advanced phishing : Smishing Vishing	• Internal attacks • External attacks	• Crypto Ransomware • Locker Ransomware	-
The biggest scams	Phish Phry attack at 2009	One coin at a time at 1996	WannaCry Ransomware attack at 2017	Cryptojacking hits Australian government websites At 2018
Targets	Individuals, especially executives: Because their information is more accessible, and they must respond to all emails. Here comes the role of the hunter in persuasion.	Organizations, particularly banks	Organizations. Because organizations contain very important information, their loss can cause significant harm to the organization	Organizations. Because the more power, the better it is. There are no stronger computers and servers than those in organizations.
The most affected country	Brazil: 21.66%	-	Indonesia: 17.10%	United States : 32%
Motivation	All attacks their ultimate goal is to get money. But in different ways.			

- **Honeypot**

It consists of setting up decoy files to attack the ransomware. Upon viewing these files, it is possible to identify the ransomware. It is possible to set up the traps or honeypot files, and wait until you are targeted. Because of this, the methodology does not require machine repair or even power for processing. Nevertheless, there is no certainty that a malware can attack the honeypot files. It is therefore important to know the file characteristics that will be targeted by the ransomware.

D. Cryptojacking attack

In this part we discuss some methods of protection against this type of cryptojacking attack. Some are embedded in browsers. Others are user responsibility.

- **Browser-level mitigation**

Several browser developers' possible mitigations include: throttling client side scripting, warning users if client side scripting uses unnecessary energy, and disabling known cryptojacking scripting outlets. Browsers like Opera took a stand against cryptojacking scripts and banned them by their blacklist "No Coin"[42].

In addition, users should remain wary of phishing emails, unknown attachments, and dubious links. And do not be the victim of these two types of attacks.

IX. TIMELINE OF THE ATTACKS

Table 1 compares some important points briefly, including target groups by attacks and motives for attacks.

X. GENERAL STATISTICS

Based on the reports published by Kaspersky, McAfee and Quick heal [43-45], we compared three attacks, phishing attack, ransomware attack and cryptojacking attack. We did not include salami slicing attack because it targets sensitive organizations such as banks as we mentioned in Table 1. It is important to hide attacks such as salami slicing attack to keep the client's trust.

Over the past three years, we note that the leading attack by a very large difference is phishing attack due to its permanent development and the diversity of methods used. In 2019, the number of attacks reached 240 million. As we note, ransomware attack and cryptojacking attack did not exceed 14 million. However, the number of ransomeware attacks in 2019 is relatively higher than that of cryptojacking attacks. Based on 2019 statistics[46]. It was noted that most of the attacks this year were criminally motivated. This general motivation is the basis of our four attacks that we discussed earlier. The percentage of cyber-crimes motivation is 84%, which is very high. This raises anxiety and fear.

Based on 2019 statistics[46], it has also been noted that the target group for attacks is individuals. This is because most network users are individuals with insufficient knowledge of the methods of protection. Unfortunately, most people do not have anti-virus software either, thus making it easier to create an attack.

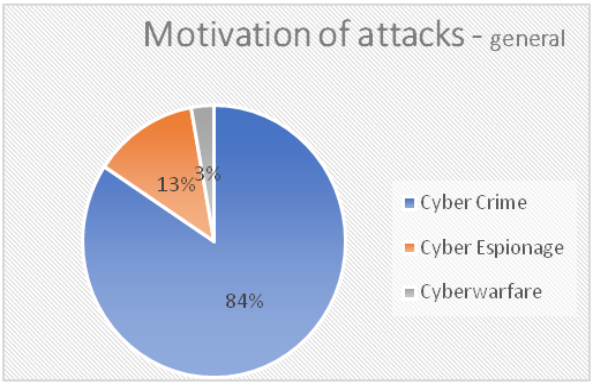

Figure 2 : Motivation of all attacks occurs in 2019

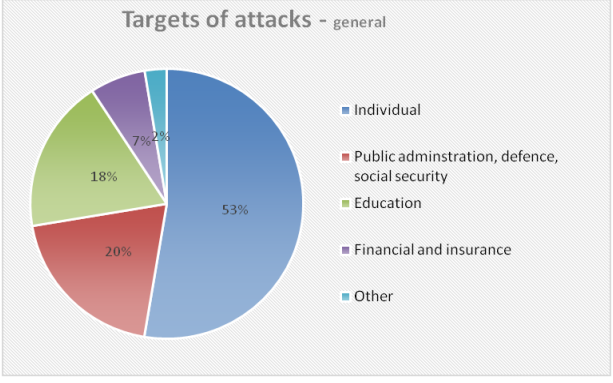

Figure 7 : Targets of all attacks occurs in 2019

Figure 3 : 10 best prepared for cyber attacks[47]

Figure 4 : 10 worst prepared for cyber attacks[47]

NordVPN c, which is a virtual private network provider, collects threat-report data from Secure list, including Global Cybersecurity Index (GCI developed by the International Telecommunication Union) scores for cyber attack readiness based on five main factors[47], as follows:

- Legal: Dealing with cybercrime by legal institutions;
- Technical: Dealing with cybersecurity by legal institutions;
- Organizational: Policies and strategies to develop cybersecurity at the national level;
- Capacity Building: Programs aimed at development, education and training in cybersecurity; and
- Cooperation: Aiming to establish partnerships and exchange information.

It was noted that those countries with the most advanced technologies have the best cyber attack preparedness. Singapore recorded the highest level followed by the United States as shown in Figure 8. Unfortunately we also have worst-prepared countries such as Vietnam and Uzbekistan as shown in Figure 9[47].

As shown in Table 3, all results indicate that these attacks are aimed at obtaining money and can even cause enormous damage to an entire country. The result explains the pivotal differences between the four cyber attack structures, but the similarity remains in the ultimate goal of getting money which is the goal of the paper.

XI. CONCLUSION

We mentioned that some of the attacks were from the eighties but became widespread with the spread of the Internet. With this spread, their types and methods have evolved to exploit all possible opportunities. We also mentioned that attacks are a battle between the attacker and the user. To win the battle the first line of defense is to know how the attacker works and then the techniques and tools needed to help prevent attacks.

We can say that cyber attacks have now become the point of concern of every individual and organization. The whole world and nations have been threatened by it. It has influenced the society and nations throughout the world, not just individuals. Because of this, the best type of security is information and cyber awareness.

Each individual must be made aware of the cyber attacks so that we can take protective action by educating the masses with the Do's and Don'ts across the network and information usage.

Table 3 : Analysis Result

	Phishing attack	**Salami slicing attack**	**Ransomware attack**	**Cryptojacking attack**
Was the goal of the first appearance is financial?	No, it was not. But later it was widely used for financial gain.	Yes , it was	Yes , it was	Yes , it was
	The origin of the attacks section			
Have the attack' ways evolved to get money?	Yes, they have. This type of attack is the most advanced.	Yes, they have.	Yes, they have.	No, they have not. Because this type of attack is still new.
	Variants of the attacks section			
Is there a similarity in work methods for getting money?	Yes, there is a very simple similarity in the strategy of working with ransomware attack	No , there is not	Yes, there is a very simple similarity in the strategy of working with phishing attack	No , there is not
	Modus operandi of the attacks section			
Did any attack cause financial damage?	Of course, it did.	Of course, it did.	Of course, it did.	Of course, it did.
	Losses due to the attacks section & Table 1			
Is it possible to protect from attack?	of course, it is .	of course, it is .	of course, it is .	Of course, it is.
	Mitigation techniques against the attacks section			

REFERENCES

1. Alzain, M.A. and E. Pardede. *Using multi shares for ensuring privacy in database-as-a-service*. in *2011 44th Hawaii International Conference on System Sciences*. 2011. IEEE.
2. AlZain, M.A., B. Soh, and E. Pardede. *Mcdb: using multi-clouds to ensure security in cloud computing*. in *2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing*. 2011. IEEE.
3. AlZain, M.A., et al. *Cloud computing security: from single to multi-clouds*. in *2012 45th Hawaii International Conference on System Sciences*. 2012. IEEE.
4. AlZain, M.A., B. Soh, and E. Pardede, *A new model to ensure security in cloud computing services.* Journal of Service Science Research, 2012. **4**(1): p. 49-70.
5. Ollmann, G., *The Phishing Guide--Understanding & Preventing Phishing Attacks.* 2007.
6. Kabay, M., *Salami fraud.* Network World Security Newsletter, 2002. **24**.
7. Richardson, R. and M.M. North, *Ransomware: Evolution, mitigation and prevention.* International Management Review, 2017. **13**(1): p. 10.
8. Carlin, D., et al., *You Could Be Mine (d): The Rise of Cryptojacking.* IEEE Security & Privacy, 2019.
9. Jakobsson, M. and S. Myers, *Phishing and countermeasures: understanding the increasing problem of electronic identity theft.* 2006: John Wiley & Sons.
10. Faragallah, O.S., et al., *Block-based optical color image encryption based on double random phase encoding.* IEEE Access, 2018. **7**: p. 4184-4194.
11. Sodhi, G.K., et al., *Preserving Authenticity and Integrity of Distributed Networks through Novel Message Authentication Code.* Indonesian Journal of Electrical Engineering and Computer Science, 2018. **12**(3): p. 1297-1304.
12. Company, A., *Cryptojacking* 2018.
13. Stephenson, D., *Spear Phishing: Who"s Getting Caught?*
14. Vaishnaw, N. and S. Tandan, *Development of anti-phishing model for classification of phishing e-mail.* Development, 2015. **4**(6).
15. Yeboah-Boateng, E.O. and P.M. Amanor, *Phishing, SMiShing & Vishing: an assessment of threats against mobile devices.* Journal of Emerging Trends in Computing and Information Sciences, 2014. **5**(4): p. 297-307.
16. Ollmann, G., *Understanding X-morphic Exploitation.* 2007.
17. RSA, *Phishing, Vishing and Smishing: Old Threats Present New Risks.* 2009.
18. Scott., A., *Salami Attacks.*
19. Alhassan, N.S., et al., *Salami Attacks and their Mitigation-An Overview.*
20. Bhardwaj, A., et al., *Ransomware digital extortion: a rising new age threat.* Indian Journal of Science and Technology, 2016. **9**(14): p. 1-5.
21. Kumar, V.S., *Cyber Crime- Prevention & Detection.*
22. BARAK, I., *HOW DOES RANSOMWARE WORK?* 2017.
23. AlZain, M.A. and J.F. Al-Amri, *Application of Data Steganographic Method in Video Sequences Using Histogram Shifting in the Discrete Wavelet Transform.* International Journal of Applied Engineering Research, 2018. **13**(8): p. 6380-6387.
24. AlZain, M.A., *Efficient Image Cipher using 2D Logistic Mapping and Singular Value Decomposition.* INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS, 2018. **9**(11): p. 196-200.
25. platform, C., *What is Cryptojacking? How it Works And How You Can Prevent It.* 2018.
26. investigation, F.b.o., *Operation Phish Phry Major Cyber Fraud Takedown.* 2009.
27. El Guindy, M.N. and F. Hegazy, *Cybercrime Legislation in The Middle East*. 2014.
28. Scaife, N., et al. *Cryptolock (and drop it): stopping ransomware attacks on user data*. in *2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS)*. 2016. IEEE.
29. Chen, J. and C. Guo. *Online detection and prevention of phishing attacks*. in *2006 First International Conference on Communications and Networking in China*. 2006. IEEE.
30. Gupta, S., A. Singhal, and A. Kapoor. *A literature survey on social engineering attacks: Phishing attack*. in *2016 international conference on computing, communication and automation (ICCCA)*. 2016. IEEE.
31. Samra, H.E., et al., *A Conceptual Model for Cloud-Based E-Training in Nursing Education*, in *Knowledge-Intensive Economies and Opportunities for Social, Organizational, and Technological Growth.* 2019, IGI Global. p. 295-310.
32. Samra, H., et al., *Utilisation of hospital information systems for medical research in Saudi Arabia: A mixed-method exploration of the views of healthcare and IT professionals involved in hospital database management systems.* Health Information Management Journal, 2019: p. 1833358319847120.

33. Alsaif, S.A., et al., *From Learning Management Systems to a Social Learning Environment: A Comparative Review and the Implications.* International Journal of Smart Education and Urban Society (IJSEUS), 2019. **10**(1): p. 1-18.
34. Samra, H.E., B. Soh, and M.A. Alzain. *A Conceptual Model for an Intelligent Simulation-Based Learning Management System Using a Data Mining Agent in Clinical Skills Education*. in *2016 4th International Conference on Enterprise Systems (ES)*. 2016. IEEE.
35. Zhang, B., et al. *An efficient image matching method using Speed Up Robust Features*. in *2014 IEEE International Conference on Mechatronics and Automation*. 2014. IEEE.
36. Singh, A.C., K.P. Somase, and K.G. Tambre, *Phishing: A Computer Security Threat.* International Journal of Advance Research in Computer Science and Management Studies, 2013. **1**(7).
37. Kumar, V.S. and A. Director, *CYBER CRIME–PREVENTION & DETECTION*. available online on: www. cidap. gov. in, 2003.
38. Alzain, M., *Image Encryption Using Chaotic Cat Mapping in the Discrete Fourier Transform.* INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY, 2018. **18**: p. 7389-7397.
39. AlZain, M.A., et al., *Byzantine Fault-Tolerant Architecture in Cloud Data Management.* International Journal of Knowledge Society Research (IJKSR), 2016. **7**(3): p. 86-98.
40. Kok, S., et al., *Ransomware, Threat and Detection Techniques: A Review*. Int. J. Computer Science and Network Security, 2019. **19**(2): p. 136.
41. S. Kok, A.A., M. Supramaniam, T. R. Pillai, and I. A. and T. Hashem, *A Comparison of Various Machine Learning Algorithms in a Distributed Denial of Service Intrusion.* 2019.
42. Pastrana, S. and G. Suarez-Tangil, *A first look at the crypto-mining malware ecosystem: A decade of unrestricted wealth*. arXiv preprint arXiv:1901.00846, 2019.
43. HEAL, Q., *ANNUAL THREAT REPORT*. 2019.
44. McAfee, *McAfee Labs Threats Report.* 2019.
45. Kaspersky, *Spam ans phishing.* 2019.
46. HACKMAGEDDON, *Cyber Attacks Statistics.* 2019.
47. Magazine, P., *Which Countries Are Best-Prepared for Cybercrime Response?* 2019.

AUTHORS PROFILE

Asalah F Altwairqi, received the Bachelor degree in Information Technology from Taif University , Saudi Arabia in 2018. Currently, she is pursuing her M.S. degree in Cyber Security at Taif University.

Mohammed A. AlZain, has achieved his PhD degree from the Department of Computer Science and Engineering at La Trobe University, Melbourne, Australia in Sept 2014. Dr. AlZain's PhD research is in Cloud Computing Security. His thesis title was "Data security, Data management, Performance evaluation for a multi-cloud computing model". He has received his Bachelor degree in Computer Science from King Abdulaziz University, Saudi Arabia in 2004, and then achieved his Master's degree in Information Technology from La Trobe University in 2010. Currently, Dr. AlZain is Associate professor in the College of Computers and Information Technology at Taif University in Saudi Arabia. His area of interest includes Cloud Computing Security, Information Security, and Distributed Systems.

BEN SOH, (S'89–M'92–SM'03) received the Ph.D. degree in computer science and engineering from La Trobe University, Melbourne, Australia, in 1995. He is currently an Associate Professor with the Department of Computer Science and Computer Engineering, La Trobe University. He had numerous successful Ph.D. graduates. He has authored more than 150 peer-reviewed research papers. He has made significant contributions in various research areas, including fault-tolerant and secure computing, and Web service

Mehedi Masud, is a Full Professor in the Department of Computer Science at the Taif University, Taif, KSA. Dr. Mehedi Masud received his Ph.D. in Computer Science from the University of Ottawa, Canada. His research interests include cloud computing, distributed algorithms, data security, data interoperability, formal methods, cloud and multimedia for healthcare. He has authored and coauthored around 50 publications including refereed IEEE/ACM/Springer/Elsevier journals, conference papers, books, and book chapters. He has served as a technical program committee member in different international conferences. He is a recipient of a number of awards including, the Research in Excellence Award from Taif University. He is on the Associate Editorial Board of IEEE Access, International Journal of Knowledge Society Research (IJKSR), and editorial board member of Journal of Software. He also served as a guest editor of ComSIS Journal and Journal of Universal Computer Science (JUCS). Dr. Mehedi is a Senior Member of IEEE, a member of ACM.

Jehad Faisal Al Amri, is a professor assistant in Computer Informatics. He graduated from the Centre for Computing and Social Responsibility at De Montfort University June - 2013. The thesis title is "An Analysis of the Influence of Cultural Backgrounds of Individuals upon their Perspective towards Privacy within Internet Activities". Currently, he is a lecturer at the Faculty of Computers and Information Technology at Taif University, Saudi Arabia.