Cyber Poison

Jemima Treesa Thomas
MS- Cyber Security
Stratford University, India Campus

Mukta Sharma, PhD
Faculty of Computer Science and Information Technology
Stratford University, India Campus

ABSTRACT
The cyber-world is developing with each passing second and one needs to know how to protect themselves from cyber-attacks as they are also growing at a much faster pace. This research paper shed light on the recent cyber-threats faced by not only the individuals, corporates, governments but also by the nations globally. The paper focuses on the top attacks which have actually changed the perspective of an attack. The attacks are not just limited to disrupting the functioning of the system, deleting some files, stealing the customers' identity or breach for monetary benefits rather it is more hazardous as these days attacks are involved in being used as a cyber-weapon. The paper also discusses about one of the most mysterious hackers that lead to the most devastating cyber-attacks in the history of the cyber-world.

The authors share how the non-technical organizations are more prone for cyber-attacks and how much badly it could affect their businesses. The author felt the need to share the prevention mechanisms through which the companies can keep them and their data confidential and secure from getting exploited by such attacks.

General Terms
Threats- Anything that results in causing a damage, modification or removal of data or a physical device is a threat.

Attacks - The attempt to cause a significant disruption from the normal way can be referred as an attack

Vulnerability- The weakness that can lead to damage if exposed can be termed as vulnerability.

Exploit – Focusing on the weakness to manipulate the data is called an exploit.

Keywords
Artificial Intelligence (AI), Supervisory Control and Data Acquisition (SCADA), Cyber-weapon

1. INTRODUCTION
Cyber is not the word of the future any more but of the present; considering all the technological impossibilities that have been accomplished. Twenty years back it was a dream to talk and see someone living on the other side of the world but the technological advancement has made the dream come true. In earlier days people used to capture & record the precious moments in albums, tapes, CDs for future reference. Now the technology has made it possible to not only capture but also share it with others immediately so that they can also be a part of that moment. This all could be possible by just a press of a button or in-short the entire world is in your palm. With internet available on a mobile phone makes the device a "smart phone". There are infinite number of advantages from the use of internet like connectivity not only among the people but now even among the devices (IOT devices), Artificial Intelligence expansions, Business Analytics, etc. There are certain shortcomings too one such weakness is in the field of security. This paper focuses primarily on cyber-attacks which is poising the cyber space.

Since ages society have seen and faced various attacks like stealing, sabotaging (destroying), stalking, espionage (spying), etc. these are traditional crimes or attacks. Cyber-attacks are rapidly increasing with the enhancement of the technology. Cyber-attacks are so powerful and harmful that they leave organizations tremble even after years of the attack. It takes good amount of time in recovering from the attacks and not to mention the cost of the damage can go up-to billions. Cyber-attack is little difficult to trace as compared with traditional attack due to anonymity it is difficult to catch hold of the culprit.

Cyber-attack is possible due to lack of knowledge with the current threats that can hamper the organization image or by being little careless. Human nature is the ultimate reason for cyber-vulnerabilities. These can be prevented by educating individuals and employees in the organization about the cyber-attacks. The employees need to know the details like why, what caused the attack, what is the motive behind the attack, who is behind such an attack, how to avoid becoming victims of such attacks, etc.

Organizations need to be more vigilant while handling highly confidential data around the internet as there are multiple vulnerabilities and a vast new section of attacks to be deployed. To ensure security, organizations should hire more cyber-security professionals who are expert in this domain. Even small companies and startups need to consider and focus on cyber-security since inception rather than leaving it for future usage as they are the most vulnerable to attacks. Attacks can be based on social engineering which includes phishing, tail gaiting, sharing confidential details about company on phone etc. and many other such attacks that lead to loss of important data or compromising important details.

2. SHADOW BROKERS
Shadow broker is a term familiar to every gamer who has played the video game series "Mass Effect". Now this term is well acquainted among the general public due to the cyber-attack that break the headlines is led by the team with the similar name [12]. According to Matt Suiche, French hacker, "The shadow broker is an individual at the head of an expansive organization which trades in confidential information, always selling to the highest bidder. The shadow broker appears to be highly competent as it trades all secrets that are bought and sold, never allow one customer of the broker to gain advantage forcing the customers to continue trading information to avoid becoming disadvantage allowing the broker to remain in the business".

Shadow brokers are considered to be a mysterious and notorious hacking group that surfaced around the year 2016. [17] They hack and breach mostly the National Security

Agency. They exploit mainly the tools and software implants from NSA and auctions them to the highest bidder causing extreme security vulnerability. [2]The leakage of one of the hacking tools from the NHS lead to one of the most disastrous cyber-attacks named as Wannacry; which affected both technical and non-technical organizations. They make their sales through a peer-to-peer encrypted network called ZeroNet. There is another advanced hacking group known by the nick name Equation Group which helps the shadow brokers for the auction and leakage.

3. CYBER-THREATS

Our civilization has grown enormously from stone-age to cyber-age. Living with the technology and enjoying the benefits and comforts of connecting with everyone on just a click of button, shopping, booking tickets, paying utility bills etc. it is helping in each domain with so much ease. Organizations are getting benefitted with the technological expansion at the same time they are more prone to cyber-attacks. With the growing technological era means more new and improved cyber-attacks. New technologies mean new vulnerabilities to exploit which is giving hackers a great provision to exploit easily a small startup or mid-size company than targeting only on big companies. [9] The lack of interest in the organizations like start-ups, small and medium companies which thinks they do not have to prioritize the need for cyber-security in the beginning and initially they don't need to employ cyber-security professionals. Unfortunately they are becoming more prone to such attack. According to Mansfield, 43 percent of cyber-attacks target small business. [9] 60 percent of small companies go out of business within six months of a cyber-attack. There is a major crunch of talented cyber-security people which leads to easy compromise in the cyber-security; making the organizations more vulnerable to attacks.

Cyber criminals are of different kind, they include financially motivated people, nation-state rivalry, political gain /issues, business feud, personal gain, revenge etc. The attacker attacks their victims with methods like malware, ransom ware, phishing, misuse of power, DDOS, SQL Injection, etc. Consequences of such attacks could include war, destroying a business, financial loss, information loss and can also ruin someone's life.

Some of the issues in cyber-security include:

1. PowerShell based attacks- The codes using power shell are complex and much harder to crack and are now used by the hackers to deploy new attacks [4].
2. Crypto jacking- The increase in profit for bit coins and other e-money are considered to be "Golden Treasures" which are now becoming one of the biggest motives of the hackers to infect more ransom ware [4].
3. Using worms to launch malware- Worms are the type of malware that has the ability to duplicate itself without any host file. This technique is now being exploited by hackers in conducting new attacks as worms help in spreading the attack faster and more efficiently [4].
4. Targeting security software- People are becoming more cautious regarding the security and hence rely more on security software. This is making attackers more focused to attack these security software organizations to deploy their attacks and to destroy their reputation and to crash the trust [4].
5. New Vulnerabilities- With the discovery of new technologies these bring up more weakness and new attacks waiting to be launched.
6. Ransom ware- The era of ransom attacks are growing owing to some successful attacks that has taken place in the past few years. It is motivating the black hat hackers to launch new ransom attacks [12].
7. AI Expansion – It has been spread like a wild fire that the cyber-security analyst will be replaced by AI. Due to the vast expansion of AI the hackers are getting their hands on such advanced technology waiting to strike the world with a destructive attack [12].
8. IOT Threats- Our new generation is growing with gadgets and to make the life easier they are relying heavily on IOT devices. [12] The more they are using IOT devices they are making themselves more susceptible to attacks.
9. Server less Application Vulnerabilities- With the use of more server-less apps the confidential information is individual's responsibility. [12] Without the right set of training or awareness regarding cyber-attacks and cyber-attack prevention to that individual can lead to the leak of such information to the wrong hands.
10. Human Nature- Humans being the most susceptible link to deploy an attack or to destroy an organization. These days because of social networking sites and carefree nature (sharing anything with anybody- especially while playing games on social networking sites) of human beings is a real matter of concern. This is being misused by the cyber-bullies for their notorious experiments.

Cyber-security as the name depict is a technique to ensure security for the cyberspace. The organizations need this practice of protecting systems, networks and programs from the digital attacks.

3.1 How these attacks affect non-technical organization?

The cyber-attacks not only affect the technical organizations but also the non-technical organizations. The non-technical organizations are also using Internet for varied tasks and they are less specialized and are unaware about the cyber-attacks. [2] One such great example is the disastrous Wannacry cyber-attack that left a huge scar for the British National Health Service. [14] Due to Wannacry attack one third of the NHS hospital trusts and around 8% of the GP practices found their IT systems disrupted. It left the systems encrypted and by no means data stored in the systems regarding the patient's medical history or the prescription could be accessed. It leads to the declaration of emergency meetings.

3.2 What are the different types of cyber-attacks?

There are different types of cyber-attacks like phishing, salami attack, Nigerian 419 scam, DOS, DDOS, SQL Injection, MITM, Cross site scripting, ransom-ware, malwares, etc. The recent attacks are making use of malwares to execute the attacks.

Malware or Malicious software's are categorized in two ways (1) Non-Resident (2) Resident as depicted in Figure 1. The

non-resident ones do not require a host to attack a system or network like Zombies and Worms. While a resident one requires a host to affect the system like Trap doors, logic bombs, Trojan Horses, viruses. Among the two, non-resident one is more dangerous as they are the one used in the recent attacks and is expected to be used in near future. As malwares spread faster through worms and zombie and is hard to identify the hacker behind the attack.

A zombie computer or in short zombie is a program that takes over another system connected via internet to launch or to initiate attacks which makes it difficult to trace back to the creator making it easy to not leave tracks. A worm is a virus that stays in the computer memory and spreads by duplicating itself; they can spread through systems connected via networks by emails or chats. One of the major issues faced by the cyber-security is the use of worms to launch malware attacks.

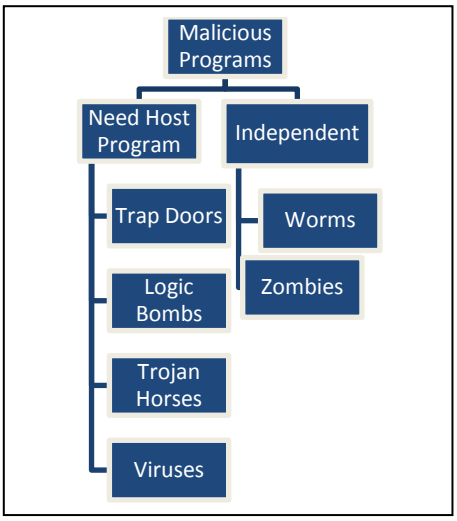

Figure 1: Malicious Software [18]

4. TOP CYBER-ATTACKS

4.1 Stuxnet

Stuxnet is a malware that is used to spread the malicious software around vulnerable weak computers. Stuxnet is also called as a worm as it shows similar characteristics of a worm. Stuxnet attacked SCADA system and target on Industrial control systems (ICS) matching the Iran's nuclear codes. [1] This was compared similar to a cyber-weapon and was aimed as an attack to Iran in 2010. A cyber-weapon is the use of technology both software and hardware for destructive purposes which leads to war between nation/states. Stuxnet was considered as the [3] forefather of cyber-weapons as it was the first of its kind which means new and improved from the previous attacks to ICS based codes that includes the involvement of nuclear power plant. Stuxnet aimed at sabotaging the centrifuges in the Iranian nuclear facility in Natanz. Till now no one has owned up to the development of the worm. [1]As per New York Times, Stuxnet was developed and deployed by US and Israel. The development of stuxnet is still hard to figure out considering it has used considerable resource, money and efforts of multiple programmers for months. They exploited four zero-day vulnerabilities to infect computers and two other vulnerabilities concerning privilege escalation.

The attack was extreme that the worm had the ability to [9] attack computers that were not connected to the internet. The attackers spread the worm using compromised USB drive as the nuclear ICS did not use the internet. A USB connected to the infected computer can affect another one when the employee handling the infected device has no clue regarding the affected worm and connects the USB to a healthy system. The attack does not take place as soon as it enters the system, it first searches the hardware, software, and settings etc. in short every nook and part of the system is checked and if it matches the code of the ICS Natanz it unleashes the payload. [1] The worm generates more new codes if the device was connected to the internet making it more dangerous. [1] The main intention of the attack was not just spying rather to remain hidden for a longer duration, and attack the main system and hides in the codes so as to make sure the centrifuge works fine in the beginning normally not raising any suspicion. Hence physical consequences were less after the attack only leaving malfunctioning centrifuges.

Later on some other malicious software's were developed using Stuxnet code one of them was named as Flames. These malwares were developed after the hackers saw the success in their attack; this was a big change in the cyber-attack method and later many such attacks were seen. Another malicious software named Duqu was developed with the code to collect information rather exploit. As new malicious software's are not made from scratch but preferred to be an updated version of an already executed malware-attack and hence the execution of this attack sparked fear to many strong nations.

Kaspersky, leading anti-virus company has always been in news especially for identifying and uncovering malware attacks like Stuxnet, Flame, Duqu etc. The UN requested Kaspersky to uncover malware that attacked an oil company in Iran and hence asked them to develop security software that would keep away such attacks in the future.

4.2 Wannacry

May 12, 2017 was the day when cyber-attack broke the headlines and affected many, the Wannacry ransom-ware was considered to be one of the most disastrous cyber-attack in the history [15] affecting more than 2,30,000 systems and 150 countries. This attack has other names like Wanna crypt or Wanna Decryptor. It attacked many multinational organizations like Renault- France, Fed-Ex, the British National Health Service and the list goes on to many universities, banks, aircrafts, railroad, US Radiology, Portugal Telecom, schools etc.

The attack mainly targeted Windows Operating system which exploited the vulnerability which was discovered by the US National Security Agency. [16]This attack was initiated primarily due to 3 factors:

1. National Security Agency, USA designed a tool named Eternal Blue to exploit the vulnerability they found in windows operating system. On April 14, 2017 the hacking tool Eternal Blue was stolen by Shadow Brokers which was auctioned and leaked and a month later the attack took place.
2. Even after the method of prevention for such attack was published it was not able to spread the awareness to the individual which increased the number of victims.
3. Initially the update was send out to only Windows 7 and above and not the older versions like XP (not supported since 2014 officially) which was used by many but did not receive any update till May 13, 2017 and ended up falling victim to the attack.

[5]Once launched Wannacry does not infect the system right away, it tries to access a hardcode URL aka "Kill Switch". If it finds the Kill Switch it does not infect the system but if it does not find the switch then the attack is initiated. [16] The attack happens after encrypting the computer data exploits the vulnerability in a legacy version of Server Message Block (SMB) in Widows. Once it attacks the system it encrypts the entire files in the system and after which it displays a message showing time and the ransom amount to be provided to decrypt the file. The SMB protocol helps various nodes on a network communicate and Microsoft implementation could be tricked by specially crafted packets into executing arbitrary code.[16] The victims get 3 days in the beginning to pay the ransom of $300 if they fail they are given 7 more days but with double the payment to be made. Still if the victims fail then the files will be deleted completely from the system. It was mentioned that even after paying the ransom many were not able to decrypt the file as the decryption code had error which ensured the data was lost and deleted. The attack spreads around other computers which were connected to the affected system through the networks. 98% of the attack was to Windows Vista, 7 and above and few on Microsoft XP.

The attack damage was severe for the British National Health Service. [13] They faced a loss of £1 million. The damage not only included the loss of money from recovering from the attack but also leads to the cancellation of 19000 appointments and had to reschedule the operations for many. The encryption of the data lead to the loss of many patients' medical history and prescriptions to be taken hence making it hard for the medical staff with the treatment. The delay for medical attention also included many cancer patients. Thankfully no life was at risk due to the attack and no personal data were leaked or stolen. We cannot expect such miracles with such lethal cyber-attacks; which can lead to be fatal to human life if no proper awareness or training is given. The importance is given to such trainings and awareness about cyber-security to non-technical organizations should be as important as the ones given to the technical organizations. [15]This attack leads to the emergency COBRA meeting which was held for the first time due to a cyber-attack.

4.3 Not-Petya

Soon after the head-line breaking attack of Wannacry another cyber-attack spread through the entire Europe called Not Petya around June 17, 2017. [13]The first victims to face the attack was Ukraine as it started as a fake Ukrainian tax software update and later on spread across Europe affecting multiple organizations, banks etc.[13] AP Moller Maersk was one of the transportation group that faced this attack drastically affecting their entire systems that lead to multiple transportation issues all in just few days. The attack was mainly focused on the Ukraine and with the codes and sources found it was later concluded that the team behind this was Telebots aka Black Energy Group or Sandworm. The major issue faced by the victims was the inability to decrypt the files even after paying the ransom. [8] After multiple searches it was concluded that this attack was more of a destructive based or a wiper and not a ransom-ware. Due to this destructive nature it might be said as a nation based attack, making the Ukrainians believe it was an attack from Russia.When the attack was first discover it was considered as the family of Petya, but later on considered as a false statement and hence was named as Not-Petya. NotPetya uses 2 most influential exploits; one was Eternal Blue and the other was an old invention named Mimikatz [6]. Eternal Blue was discussed earlier also in the paper a tool created by the US-NSA for taking benefit of a weakness in windows protocol; which was leaked in 2017 allowing hackers to remotely run their code on any unpatched system. Mimikatz, was invented in 2011 by French security researcher Benjamin Delpy. He revealed that Windows users' passwords are left lingering in computers' memory. After hacking the system, passwords could be pulled out of RAM and can be used to get into other machines accessible with the same credentials. Mimikatz & EternalBlue is a lethal combination. Hacker can infect system which is not patched and grab the passwords from them to infect other systems that are patched.

[11]The attack does not take place as soon as it entered the system, it first checks if the system has been under attack previously as to confirm if the system is immune or not. The check is done by looking for a file named perfc.dat which acted like a kill switch and initiated the attack to systems without the file perfc.dat or the systems that has changed the name of perfc.dat to perfc or some other name. [11] After checking for the kill switch the attack quickly moves to the next step of opening the logical volume encrypt the data stored by over writing the first sector of the volume and then checks if Kaspersky flag is set and the overwrite the code. After this it forcefully dismounts the volume and overwrites the drive. After this the system gets shutdown automatically.

[12]The attack had great impact on AP Moller Maersk group as the quick shutdown after the attack made the IT department panic for 2 hours and after the employees were advised to leave their cubicle and to completely turn off their system making their digital phones useless as well as it was connected to the network. [11] As mentioned before even the ransom couldn't decrypt the code as no key existed to decrypt the files that got encrypted. Globally the attack brought around $10 billion in total damages. The attack that occurred a month before Wannacry which was considered as one of the disastrous did not cause much damage and cost $4 billion and $8 billion for the entire damage.

5. HOW TO PREVENT SUCH ATTACKS?

By each passing day the attacks are increasing. Therefore, it is important to spread awareness about such attacks and also to train each individual from being falling into the trap and become a victim of such attacks. Following steps will keep an individual away from attacks:

1. The basic necessity is a good complex, strong password. It should be minimum 8 characters long with a mix of uppercase, lower case, alpha numeric components and special characters.
2. Updating the Operating System when an update is available can be a good start.
3. Having a backup for important files or storing them in the most casual way can help the user from paying the ransom as well as to keep their data secure.
4. Enabling file history system protection
5. Use of One Drive for consumer or business purposes.
6. Use of Microsoft edge for smart screen protection.

   Disable the RDP feature as much as possible and only use them when needed.
7. Multifactor Authentication methods.

8. Not activating any viruses by downloading or opening unknown or unauthorized software or mails.
9. Educating the employees of an organization about the cyber-attacks, social engineering cases and how they are done through phishing, un-safe software.
10. Installing anti-ransom ware software.
11. Keeping the anti-virus and firewall software up to date.

6. CONCLUSIONS

As it gets clear on how advanced the attacks happened and how they can be used for mass destruction injects fear in us, but to know that we can prevent such attacks to a certain extend calms our nerves as well. It is all about taking all the right precautions while handling the fragile information around the internet. From the top cyber-attacks one can see that none of the attacks initiates as soon as it enters the system instead looks for codes or kill switch and only attacks the systems that does not have this long URL or the vaccination. Proper back up system, the right use of the device by not opening up or installing unauthorized or unknown software or mails with unknown attachments, proper use of firewalls and anti- virus software's installing security software etc. Making sure that the non-technical organizations pays attention to cyber-attacks as important as the IT sector takes it to minimalist the damage, be updated about the technological advances these are few of the precautions that can be taken in-order to stay alert with the security.

7. REFERENCES

[1] Baezner, M, Robin, P. 2017. Hotspot Analysis: Stuxnet. *Retrieved From:* https://www.researchgate.net/publication/323199431_Stuxnet

[2] Brandom, R. 2017. UK hospitals hit with massive ransomware attack. *Retrieved From:* https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin

[3] Denning, D E. 2012. Stuxnet-What has changed. *Retrieved From:* https://res.mdpi.com/futureinternet/futureinternet-04-00672/article_deploy/futureinternet-04-00672.pdf?filename=&attachment=1/

[4] Dolly, J. 2017. Top 5 cyber security concerns for 2018. *Retrieved From:* https://www.csoonline.com/article/3241766/top-5-cybersecurity-concerns-for-2018.html

[5] Fruhlinger, J. 2018.What is WannaCry ransomware, how does it infect, and who was responsible? *Retrieved From:* https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html

[6] Greenberg, A. 2018. The Untold story of NotPetya, The devastating cyber attack in history. *Retrieved from* https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[7] Guta, M. 2018. FBI Warns of Hackers Using Remote Desktop Protocol, Is Your Business at Risk? *Retrieved From:* https://smallbiztrends.com/2018/10/rdp-hacking.html

[8] Inanov, A., Mamedov, O. 2017. ExPetr/Petya/NotPetya is a Wiper, Not Ransomware. *Retrieved From:* https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/

[9] Kushner, D. 2013. The Real Story of Stuxnet. *Retrieved From:* https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

[10] Lin, M. N.A. Cybersecurity: What Every CEO and CFO Should Know. *Retrieved From*: https://www.toptal.com/finance/finance-directors/cyber-security/

[11] LogRhythm Labs, The Security Intelligence Company. 2017. NotPetya Technical Analysis. *Retrieved From*: https://logrhythm.com/pdfs/threat-intelligence-reports/notpetya-technical-analysis-threat-intelligence-report.pdf

[12] Mason, J. 2018. 5 Cybersecurity Challenges and Trends: What to Expect in 2018. *Retrieved From*: https://www.globalsign.com/en-in/blog/cybersecurity-trends-and-challenges-2018/

[13] Newman, L. 2017. The Biggest Cyber Security Disaster of 2017 So Far. *Retrieved From* https://www.wired.com/story/2017-biggest-hacks-so-far/

[14] Palmer, D. 2018, This is how much the WannaCry ransomware attack cost the NHS. *Retrieved From:* https://www.zdnet.com/article/this-is-how-much-the-wannacry-ransomware-attack-cost-the-nhs

[15] Palmer, D. 2018. WannaCry ransomware crisis, one year on: Are we ready for the next global cyber attack? *Retrieved From:* https://www.zdnet.com/article/wannacry-ransomware-crisis-one-year-on-are-we-ready-for-the-next-global-cyber-attack/

[16] Rouse, M. 2018. WannaCry ransomware. *Retrieved From:* https://searchsecurity.techtarget.com/definition/WannaCry-ransomware

[17] Schneier, B. 2017.Who Are the Shadow Brokers? What is—and isn't—known about the mysterious hackers leaking National Security Agency secrets. *Retrieved From:* https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778

[18] Stallings, W. 2005. Cryptography and Network Security Principles and Practices. Prentice Hall. 4th edition. /