WannaCry Ransomware and its impact on the UK's National Health Service

Rami Akrem Addad[1], Oussama El Marai[1], Hamed Hellaoui[1], and Ibrahim Afolabi[1]

[1] Aalto University, Espoo, Finland

Abstract

Crimes are committed almost on daily bases in different parts of the world and cybercrimes are not an exception. Cybercrimes and Cyber attacks are and will continue to be the source of major challenges facing the ever-evolving and developing human society. Having practical cybersecurity approach and guidelines in dealing with these challenges is not only a want but a necessity for every organization, company, industrial sectors, and government ministries. There is a need for nations to raise their level of cybersecurity awareness and preparedness and identify their critical infrastructure in the event of a cyber attack in order to know how best to respond. There are various forms of cyber attacks, from Distributed Denial of Service (DDoS) attack to malware or even Phishing attack, all these forms of attacks are carried out within the cyberspace, on different levels of magnitude and motivations. One of the types of cyber attack mentioned above, precisely, a malware attack was launched against the computer and communication infrastructure of the entire world. The malware named WannaCry was used to attack several institutions around the world by exploiting the security vulnerability of the Windows operating systems. The aim is to encrypt the users' files and lock out their devices and ask for a ransom to decrypt the data basically to make money. In this article, we will be discussing cybersecurity and cyber attack and its different forms. Most importantly, we will focus on the malware attack on the UK National Health System (NHS), its impact, and recovery and then finally provide some suggestions on the way going forward.

Index Terms

Cybersecurity, Ransomware, WannaCry, and Data Security, National Healthcare Service (NHS).

I. Introduction

Data security is a major aspect of cybersecurity that deals with the process of protecting digital data throughout its lifecycle from unauthorized access that could bring about unwanted actions which may lead to data corruption, theft, destruction or manipulation/modification. Protecting data from authorized access in this case simply imply securing important and confidential data of users from any potential cyber attacks. Cyber attacks on the other hand, often do not happen randomly, there is usually a reason, some form of motivation behind its eventualities. A cyber attack could take place simply for any of the following reasons: Espionage; just to take control of a system and show off about it; just to disrupt a peaceful process as a way of protest, otherwise known as Hacktivist; some may just hack a system for catching fun; others do it for stealing valuable information; and some do it only for testing the security vulnerabilities of usually big and popular organizations.

When a cyber attack happens, it is usually as a result of something not properly done to secure the network and communications infrastructure well enough against any form of security vulnerabilities. As such, the potential attacker takes advantage of this loophole, depending on the type of attack to perpetrate the intended malicious act. Notwithstanding, the individuals, organization or company whose system has been attacked will often pay either in valuable time or money.

Lately, there has been a rapid increase in the rate at which acts of cyber attacks are being carried out. While many go unnoticed, a handle full of them was reported and those with major impacts have caught the attention of the media. One of such reported incidences of cyber attacks in the last few years is the WannaCry Ransomware that affected almost the majority of institutions exploiting a breach in older windows systems. In general, ransomwares are a type of malicious software that find their way to the computers of individuals or organizations, take control of them without necessarily having the right privilege and then threaten to use the content of the machines wrongly except a ransom is paid.

Among victims that were targeted by the WannaCry ransomware, there exist use-cases that specifically attracted our intention due to their sensitivity. The breach in the security of the NHS system in the United Kingdom is a prime example of these cases. WannaCry happened on a massive scale and affected a significant segment of the network architecture of the NHS system.

It swept across the computer networks of at least eighty NHS Trust hospitals, taking absolute control of their system. The ransomware managed to have access to the file systems, encrypt them and then demand a ransom before it will be decrypted.

Based on the critical observations, the contributions of this paper are:

- A brief Introduction on ransomwares' types and manner of behaving in general perspectives.
- A detailed explanation of how WannaCry affected various organizations and how to overcome such an attack.
- A comprehensive study of the NHS institution while emphasizing the majority of prevention, reaction, and mitigation methods employed to overcome WannaCry.

The remaining of the document is organized as follows. Section II provides some motivations and background on cybersecurity. Section III presents a particular type of cyber attack, which is a ransomware attack. WannacCry ransomware attack is detailed in Section IV. Thereafter, Section V presents the impact of this attack on a specific institution that represents our case study. Finally, Section VI concludes this documents.

II. Motivation & Background

In this section, we will discuss the fundamental aspects of cybersecurity, provide answers to why organizations, firms, government ministries or even an entire nation should be careful attention toward ensuring that their cyberspace is secured.

Over the past decade or more, cybersecurity has often surfaced as one of the most discussed hot topics in the media. In fact, one of the most sought after information technology experts in the world are those who specialize in cybersecurity. This concept is so important that companies around the world are not just hiring cybersecurity experts but also making them as part of the nucleus of the companies board members. With the surge in the activities that goes on online, it is almost natural that there will be a corresponding move from malicious cyber domain users to undermine and disrupt the peaceful conduct of online activities. The reality is that we will always have them around us, and we have to always be prepared for their sinister acts.

However, to prepare for them, we need to understand in comprehensive details what exactly is cybersecurity, against what sort of cyber attacks should we secure our systems and finally, what are the reasons why we are targeted.

A. *What is Cybersecurity?*

As much as one would love to have a straightforward answer to this question, the topic is obviously broader in scope than one with a single answer. Nonetheless, by considering as many aspects of it as possible, we have come up with the following definition. Cybersecurity is a science that defines the standards, policies and best-practices to protect (prevent, detect, stop, recover, misuse) software and hardware assets (digital data and physical infrastructure) operating within a cyber environment against unauthorized access, which may lead to malicious actions (corruption, theft, destruction or manipulation/modification, service disruption) in order to preserve data availability, confidentiality, integrity and possession throughout its lifecycle (from source to destination and in-between) from both inside and outside attacker.

B. *Types of Cyber attacks*

- DDoS - is a form of attack targeted towards a network or server to disrupt the flow of traffic especially going to it by overwhelming it with a flood of internet traffic by effectively using multiple compromised nearby computers as the source of the traffic.
- MitM - (Man in the middle) a type of attack where the attacker relays the communication between two parties.
- Eavesdropping attack - is the act of listening to communication without authorization.
- Phishing - an attempt of obtaining sensitive information by making the victim believing she is addressing to a trusted party.
- SQL injection attack - it targets databases by injecting SQL codes.
- Drive-by attack - is a form of malware spreading attack whereby the attacker plants a script for perpetrating a malicious act on a website with the name of known software and then an innocent user downloads the malicious software hoping it was the intended one.
- Password attack - is a process by which the password of an individual is recovered from a storage or while in transmission, especially when it is so done transparently.
- Cross-site script (XSS) attack - is a form of client-side code injection, which is done by a malicious user through a trusted website that uses a one time trusted login to authenticate users across all the pages served by it.
- Malware attack - is a form of attack in which malicious softwares find a way to get into the victims' computer to perform unauthorized activities.

III. RANSOMWARE

A. What is a Ransomware?

Ransomware attacks form a particular case of security threats as it involves both the employment of cryptography in case of crypto ransomware and network security. It is a type of malware that prevents users from accessing their data and threatens to publish, delete or destroy it unless a ransom is paid. It is noticed that there is no guarantee for recovering defective data after paying the ransom. The fact that each ransomware has a unique way of propagation makes them hard to counterattack and mitigate, thus the robustness of the threat. It is worth notice that initial ransomwares were based on simple symmetric encryption making them easy for decrypting. Nonetheless, in the case of recent crypto-ransomware, the threat can be either not following math-based cryptography or based on asymmetric keys which results in inconceivable reverse engineering.

B. Types of Ransomware

Ransomware is a general term derived from asking for a ransom after kidnapping worthy items. However, different manners of kidnapping can be observed, thus the existence of several types of ransomware. The two main varieties are:

1) Locker-based Ransomware: Locker ransomwares are generally the less damaging threats. Locker-based ransomware starts by locking users' computers and displaying an official message stating the ransom's demand. "Reveton" is a prime example of such type of ransomware. However, this type is not that peaceful as in many occasions it turns out to be a real threat when including password-stealing software in addition to the continuous blackmailing and illegal activities.

2) Crypto-based Ransomware: The appearance of the first Crypto-based Ransomware "Cryptolocker" in 2013 marked a radical change in criminals' tactics. Crypto-based Ransomware does not just block access and send a ransom demand, but it encrypts also many types of users' files based on the randomized generation of symmetric/asymmetric keys, this process may differ based on the followed strategies. Usually, making data recovery is almost impossible thus paying only help and encourage the development of much-sophisticated security threats. In addition, this kind of attack can lead to the creation of backdoor access and allows illegal access to attackers.

It is noticed that WannaCry forms an advanced version of Crypto-based ransomware that exploits both the usage of keys and network domain to spread the attack over the world.

IV. Case Study: WannaCry Ransomware

A. General description

WannaCry is a ransomware attack that marked the year 2017. The attack targeted computers running Microsoft Windows OS (including Windows XP, Windows 7 and Windows server 2003) and was designed to block access to data by encrypting them. The WannaCry ransomware was also qualified as worm as it could spread through across computer networks. A ransom notice was displayed in the infected computer demanding the users to pay $300 within three days (or $600 within seven days) in Bitcoin to decrypt the files, as shown in Fig. 1. The damages caused by the attack are estimated to billions of dollars. Despite no hacker group has claimed the attack, it is believed that the ransomware was originated by North Korea [1].

Fig. 1. Infected computers were displaying a notice demanding users to pay in Bicon to decrypt the files.

WannaCry exploited a vulnerability which was present in Windows implementation of Server Message Block (SMB) protocol. According to different sources, this vulnerability was already discovered by the NSA (US National Security Agency). However, the latter developed a program to exploit it rather than reporting this issue to the community. This program, called EternalBlue, was after employed by WannaCry to gain access to the systems. According to Microsoft, the

firm has discovered the vulnerability a month prior to the beginning of the attack and has issued a patch. However, many systems were not patched the day the attack took place. The spread of WannaCry was very noteworthy, especially at the beginning, as it could strike a high number of computers. Within one day, it was reported that more than 230,000 computers were infected in over 150 countries. Fig. 2 shows a map of the countries initially affected by WannaCry ransomware. Thousand of organizations were impacted by the attack, including 30 to 40 publicly named companies such as Britain's NHS, the Russian Interior Ministry, Telefonica (Spain's largest telecommunications company) and FedEx. The case of NHS was been widely reported in the media, as per the critical nature characterizing this structure. About 16 of the 47 NHS trusts has been affected and different main functionalities have been disturbed (e.g. routine surgery, doctor appointments, etc.). 40,000 organizations have been affected in China, including 60 academic institutions [2].

Fig. 2. Countries infected by WannaCry ransomware.

Although it is not known how the initial infection has begun, but it is highly believed that the threat was initially spread through emails. The impacted organizations were using systems which did not apply the patch issued by Microsoft. Once discovered, the attack was mitigated within few days, as Microsoft has raised the priority of updating the systems and installing the patch. Additionally, the way the worm was working allowed the use of a kill switch to prevent its spread. There has been a huge consensus among experts that paying the ransom is not the correct way to hand this issue. Indeed, there were no guarantees that users will get their data back after the payment. In addition, more revenues for the attackers would encourage them to continue in this direction and carry out more attacks. Despite the advice of the experts, the

bitcoin related to the ransomware received a considerable amount (about $130,634) from the victims to get their files back, but often without vain [3].

B. WannaCry, how it works?

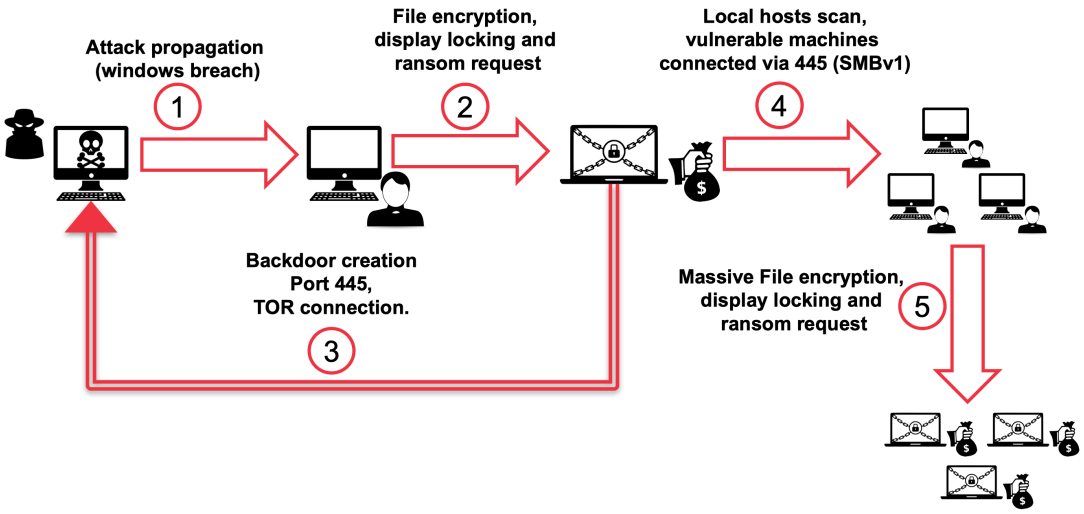

Fig. 3. Anatomy of WannaCry.

Fig. 3 depicts a brief description of how the WannaCry ransomware infected millions of devices and computers around the globe. For the sake of simplicity, deep technical details are omitted. Initially, we assume that the attacker somehow exploited the windows's security breach to enter the victim's computer. Then, the user's files will be encrypted using AES-128 cypher followed by a display locking and a ransom request. This process block access to any information within the users' computers. Taking advantage of the blockage caused by WannaCry, the attacker profits for creating backdoor access hidden via the ToR network to keep the anonymous control over the user's machine. Meanwhile, the attacker avail and open the port 445 which was supposed to enable a local sharing via the usage of the SMBv1 protocol. By opening both the backdoor and the SMBv1 port, the attacker will be able to locally scan vulnerable machines connected via the port 445, allowing simultaneously a massive propagation of the attack over all the local hosts. The ransomware propagation was shown within one local domain but scaling the attack surface will result in huge damages.

C. WannaCry, how to overcome it ?

In this manuscript, the WannaCry attack against the National Healthcare Service (NHS) is explicitly examined, however, as introduced earlier, WannaCry affected almost all societies' parts. Before deep diving into the NHS case study, we introduce common precautions and practices that allowed to overcome WannaCry's danger in a global sphere. The mitigation plan is designed from three levels recommendations and perspectives. The first and the basic level of recommendation is related end-users, this level is known to be the most vulnerable point due to the lack of knowledge for usual working users. The two remaining ones are linked with technical levels and related to Company-level and IT administrator recommendations respectively. Those two last levels portray the executive part in charge of handling massive security breach like WannaCry. In what follow each recommendation level will be profoundly discussed.

1) End-users recommendations: Generally, companies, national institutions, and associations dispose of various types of employees as well as many distinct departments. Thus, a bunch of workers is responsible for cybersecurity incidents while the remaining employees have other qualifications. However, normal workers must follow best practices in case of cyber threats such as:

- Creating a backup of all the data on an encrypted, removable external device (e.g. cloud, hard drive) after ensuring being disconnected from the internet;
- Ignoring attachments, unauthorized software, and publicities from unknown sources;
- Informing IT administrators whenever a suspicious activity is perceived (e.g. the appearance of a new folder, hard drive or text file)

2) Company-level recommendations: The company-level assure external coordination and collaboration as in general serious threats require even an international. consensus. Upon receiving threats notification from the IT administrators, the company engages critical decisions to handle the attack. This process is not only employed in crises, but it may also be applicable for precaution plans where the company buy some anti-malware as well as anti-virus from security vendors based on a request from the IT stuff.

3) IT administrator recommendations: IT administrators are responsible for coordinating between the company and its workers in addition to technically mitigating threats and guarantying the fastest reaction possible. The mitigation actions related to WannaCry can be summarized in:

- Blocking port 445 that serves for transferring files over the network using the SMBv1

protocols.

- Ensuring the patching of all Windows OS and Microsoft software (i.e. MS17-010 patch), while upgrading outdated operating systems and blocking SMBv1 protocol.
- Notifying all employees to not open unknown attachments and emails as the latter was considered as one of the first vectors of propagation of the WannaCry ransomware.
- Monitoring and scanning all file exchanged over the network as WannaCry is also considered as a warm in its way of propagation.
- Revising all users' privileges, prevent their escalation and restricting write actions over the network to prevent any propagation.

V. The Impact of WannaCry on National Healthcare Service (NHS)

A. About NHS

The NHS is the public health care in the UK that provides most of the healthcare services such as primary care, dentistry, and ophthalmology. Initially, it was formed in 1948 and primarily funded by the government. Then, largely supported by National Insurance payments and general taxation. The NHS provides free healthcare services to almost anyone registered in the system including all UK citizens and legal residents.

To provide better services to NHS patients and support local systems, seven regional teams were created namely: East of England, London, Midlands, North East and Yorkshire, North West, South East, and South West teams. Essentially, the responsibility of these teams cut across quality, financial and operational performance of all NHS organizations.

Recently, NHS England and NHS Improvement (another healthcare body that is responsible for the patient safety, high quality and compassionate care) started working closely to deliver the best possible services to their patients. Ultimately, they aim at fostering the culture of support and collaboration through the following aspects:

- Improving the patient's data quality in order to provide better services.
- Promoting accountability at different healthcare bodies for adopting standards and best practices.

NHS was a victim of an attack by WannaCry ransomware during the period from May 12th to 19th May 2017. Historically, some of the NHS trusts were targeted individually by cyber attacks (ex: Barts Health NHS, Northern Northern Lincolnshire and Goole NHS Foundation Trusts in 2016), but WannaCry attack is considered as the largest cyber incident ever seen by

NHS. An investigation conducted by the National Audit Office (NAO) revealed that NHS was warned about cyber attacks one year before the attack. The warning report mentioned that cyber attacks may compromise patients' data. It also requested from the different healthcare bodies to take practical actions towards securing their cyberspace including migrations to newer operating systems. In what follows, we provide a summary of the vulnerabilities and precautions taken by the NHS. Next, we talk about the affected parts in NHS England, followed by the actions taken to respond to the attack. Lastly, we conclude this section by the lessons learned from WannaCry attack. It should be noted here that almost all information given in this section was summarized from the NAO's investigation [4].

B. NHS precautions before the attack

Three years before the attack, and precisely in 2014, a written letter has been sent to the different trusts asking for a migration plan from old software and operating systems by maximum April 2015. The Department of Health took also the following measures to improve the cybersecurity in the NHS:

- Diffused alerts concerning cyber threats.
- Provided a hotline to be used in case of cyber incidents.
- Shared best practice procedures.
- Conducted on-site assessments to measure the readiness of the NHS trusts.
- Implemented the 10 Data Security Standards recommended by the National Data Guardian.
- Reinforced its teams by providing them with multiple training to deepen their skills in cybersecurity.
- Raised the awareness of their staff about cyber threats.

C. NHS vulnerabilities

Even though all these measures and precautions, it seems that these measures were not sufficient to protect the NHS trusts from WannaCry ransomware. Indeed, the investigation conducted by the NAO revealed that the NHS department's response was one year late (in July 2017, i.e. after the ransomware attack). This raises many questions on how efficient was the NHS implementation of the aforementioned precautions. Indeed, the NHS department conducted on-site assessment on 88 trusts out of 236 just prior to the attack to check if they correctly implemented the provided guidance and effectively applied its advice. Specifically, they recommended

patching a critical issue in their systems. Unfortunately, no trust had passed the test. Specifically, the investigation revealed that there was some devices in th infected organisations were running unsupported operating systems such as Windows XP. Also, there were other infected devices that were running supported but unpatched OS. Another vulnerability was identified in the firewalls since they constitutes the first systems' defense of the NHS organisations. If these firewalls were strong enough, it does not greatly matter whether the systems behind were patched or not.

D. What are the affected parts in NHS?

As mentioned previously, the WannaCry cyber attack is considered as the most harmful attack ever seen or experienced by the NHS due to the caused damages. The report delivered by NAO revealed that NHS England does not exactly know the full extent of the disruption, but they mentioned that at least 34% of the trusts had been affected. Precisely, it was reported that 80 out of 236 trusts across England were affected, whereas 34 were infected, meaning that the devices were locked out and the files were encrypted, and 46 experienced service disruptions. For the latter, they promptly shut down their devices once they knew about the attack to avoid spreading the ransomware, and they continued performing their daily activities using papers. It should be mentioned that the term affected include both infected organizations and those experiencing disruptions.

Additionally, the NHS Digital identified 71 organisations and 21 trusts trying to contact WannaCry domain during the period from 15 May until 15 September. Also, 603 primary care and organizations belonging to NHS were also reported as infected by the attack. This statistics does not include organizations sharing data with infected trusts.

As to the disrupted services, the report mentioned that the NHS England had estimated that over 19000 appointments had been cancelled. This is apart from the number of General Practitioner (GP) appointments cancelled and the diverted ambulances and patients. In fact, five different areas (London, Essex, Hertfordshire, Hampshire and Cumbria) were seriously impacted, and the patients in these areas had to incur travels to other healthcare centers. It was also reported by the NAO that the NHS England believes that no data was compromised or stolen. So, the major damages caused by the attack were the service disruptions. It was reported that medical devices such as MRI scanners, Radiology and blood testing devices were not away from the cyber attack. They was indeed isolated in purpose to avoid them being infected, which caused

service disruption too. Fig. 4 summarizes the different kind of known and unknown disruptions caused to NHS England.

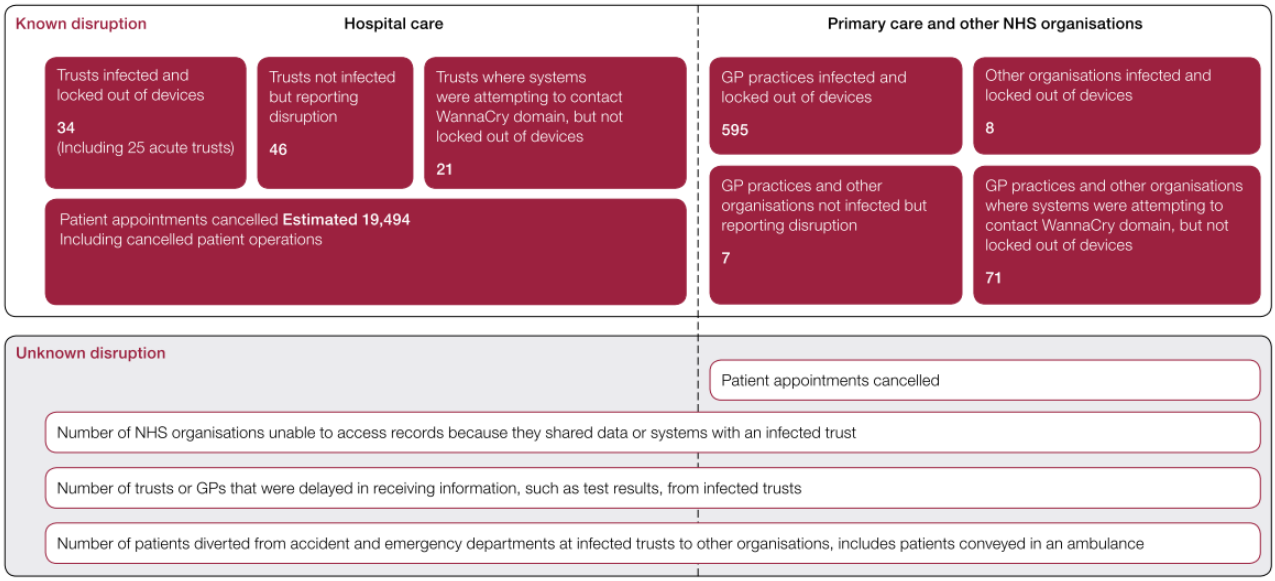

Fig. 4. The impact of WannaCry attack on NHS England.

Regarding the financial losses resulted from this attack, the NAO report didn't talk about any numbers. However, some of the top prominent newspapers such as The Telegraph [5] published in 2018 that this attack costs £92.

It was also reported that, fortunately, the IT's systems wasn't affected by the attack. This might be due to the level of awareness of the IT team and their implementation of the safety measures. Furthermore, usually the IT team uses the latest operating systems and they are eager to maintain their systems up-to-date. This keeps them safer than the others who don't follow this good practice.

E. How NHS national bodies responded to the attack?

In order to minimize the damages caused by WannaCry attack, the NHS responded as follows:

- It advised the infected trusts not to pay the ransom.
- A cybersecurity researcher belonging to NHS has activated "kill-switch" on the evening of the same day of the attack to stop the WannaCry ransomware from spreading. This helped a lot in protecting other trusts and systems.

- Following this attack, the NHS department created a plan for national and local organisations. This plan defines how these organisations should respond to cyber attacks.
- Local organisations reported to many organisations including the police. This is due to either a lack of a clear plan to follow in such situations or the plan exists but the staff members are not well trained on the execution of this plan.
- It applied its major incident procedures.
- It focused on ensuring and maintaining emergency services.
- The NHS trusts' staff worked extra hours and during the week-end to enter into the system the data that was registered on papers.

F. Lessons learned from the attack?

The investigation conducted by NAO after the WannaCry attack revealed many violations and issues that are not very hard to implement, but when discarded they led to important service disruptions and financial losses. This cyber incident helped learning many lessons that, when correctly implemented and taken into consideration, could keep the cyberspace secure and prevent from detrimental effects. In the following, we summarize some of the learned lessons from the NHS breach by WannaCry ransomware.

- From the fact that the NHS's IT systems (usually they use latest OS, not the old ones such as XP) weren't impacted by the attack, this shows the importance of raising up the level of awareness of every employee and rigorously follow the guidelines and best practices, and properly implement the safety procedures.
- Upgrading to the latest systems, installing antivirus and keep them up to date is highly important. This should be an automatic process forced by the IT team, not a choice that might be accepted or declined by the employees.
- Assessing the implementation of the CareCERT emails sent by the Boards.
- It is extremely important to have a strong firewall that protects the systems.
- There should be a clear plan that every employee should be aware of and well trained on how to trigger and execute it.
- Maintaining a communication channel(s) between the NHS organizations during the attack.
- The NHS has pumped an additional $\pounds 21$ million to the cybersecurity budget.

VI. Conclusion

The evolution in technology and cyberspace is associated with development in cyber attacks. As presented in this document, there are different types of cyber attacks. Ransomware particularly cause lot of damage as they are used as tool for blackmailing. In addition, as the attackers can get money, they will continue developing in their attacks. The studied case, WannaCry ransomware, showed that such attacks can have an effect on the entire planet. Moreover, sensitive sectors can be impacted, as it was the case for the UK' National Health Service. In the other hand, despite the fact that the ransomware has exploited a vulnerability in the used systems, the patch to fix this problem was issued one month prior the beginning of the attack. Almost all the systems which had been patched were not infected by the attack. The first step to protect against such attacks is to adopt practical cybersecurity guidelines.

References

[1] "What is wannacry ransomware, how does it infect, and who was responsible?" https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html, accessed on May 14, 2019.

[2] "Ransom.wannacry," https://www.symantec.com/en/uk/security-center/writeup/2017-051310-3522-99, accessed on May 14, 2019.

[3] "Two years after wannacry, a million computers remain at risk," https://techcrunch.com/2019/05/12/wannacry-two-years-on/?guccounter=1&guce_referrer_us=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_cs=GYOOuEtEBnJiQGjW3JYofQ, accessed on May 14, 2019.

[4] "Investigation: Wannacry cyber attack and the NHS," https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf, accessed on May 14, 2019.

[5] "The telegraph," https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/, accessed on May 14, 2019.