Chapter 5
Cyber-Physical Attacks and the Value of Healthcare Data: Facing an Era of Cyber Extortion and Organised Crime

Jaime Ibarra, Hamid Jahankhani, and Stefan Kendzierskyj

Abstract Cybercrime has reached to a level that any cyber-attack can cause great levels of extortion. With the support of technology, healthcare organisations have been able to enhance medical treatment assuring better solutions to improve life-style of people. Likewise, criminals are attracted to the information allocated within hospital and clinics regardless of physical or digital storage. Electronic Health Records (EHR) are the most important asset in healthcare and criminals are aware of their value in the black market, including the dark web. This paper analyses the impact of cyber-attacks to healthcare organisations including methods used by criminals to enhance their anonymity, and the value of healthcare data nowadays. It studies blockchain, The Onion Router (TOR) and other common tools to ensure security and privacy while navigating through the internet and the reason why cybercriminals take advantage of the dark web to sell stolen information from hospitals in order to get higher financial gain. It also looks at the levels of extortion that is caused to organisations and how people are compromised.

Keywords Cybercrime · Cyber attack · Electronic health records · EHR · TOR · Blockchain · Virtual private network · Proxy · Anonymity · Extortion · Dark net · Black market · Personal identifiable information · PII · Internet of things · Cloud computing · Deep web · Dark web · Attacker · Clinical trial · Medical treatment · Endpoint security · Network security · Ransomware · Information theft · Denial-of-service · Cryptomalware · Cryptocurrency · Cryptomining · Track covering · Encryption

J. Ibarra · H. Jahankhani (✉) · S. Kendzierskyj
London Campus, Northumbria University, London, UK
e-mail: jaime.jimenez@northumbria.ac.uk; hamid.jahankhani@northumbria.ac.uk; Stefan.Kendzierskyj@northumbria.ac.uk

H. Jahankhani et al. (eds.), *Blockchain and Clinical Trial*,
Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-030-11289-9_5

5.1 Introduction

A cyber-attack is a daily risk that organisations must deal with, which involves financial, organisational, technological and reputational threats causing damage and/or disrupting services. The world is facing an era where most of criminal performance and activities are being executed through the internet and organisations are struggling to find out the most optimal solution to protect the cyber security of their infrastructure along with their most critical assets. Technology is located everywhere and it provides a great support in businesses where data has become the most important asset due to the sensitivity of the information trusted by customers, partners and regulatory officers. On the other hand, implementation of Information and Communication Technology (ICT) infrastructures has allowed cyber criminals to perform malicious actions, where the scope is currently speculated as limitless along with all the infinite opportunities to break into computer systems and machines without authorisation.

The healthcare sector has adopted sophisticated network infrastructures and allowed to integrate machines into their systems. This term is known as Cyber-Physical Systems (CPS) and enhances the performance of medical treatments offering better lifestyle options to patients. Thanks to the Internet of Things (IoT), cloud computing, along with other cutting-edge technologies such as Artificial Intelligence (AI), Machine Learning (ML), Data Science, Bio-telemetry, Virtual Reality (VR), the medical sector has shown a noticeable evolution reaching to the point of using nanotechnology to perform highly complex and dedicated surgeries. In addition of these advancements, the implementation of Electronic Health Records (EHR) systems has contributed to hospitals, clinics including trials and research to have immediate access to information regarding patients. This includes people that can reach to this information from any device that has access to a network with internet connectivity, thanks to the deployment of wireless networks such as Wi-Fi. Nowadays, it is possible to monitor in real-time health, the conditions of patients without having a doctor or nurse watching over the person 24/7 thanks to the deployment of portable and wearable devices giving the nomination of Wearable Body Area Networks (WBAN). These networks transmit information regarding the condition of a patient to cloud environments, processing tons of data every second and where possible, sending notifications to general practitioners or specialists in case of any abnormal behaviour. The design, configuration and deployment of electronic devices has changed the landscape of healthcare compared to traditional paperwork, which involved lots of time spent at the hospital taking basic tests such as blood tests, heartbeat, blood pressure, etc. Likewise, it has attracted organised cybercrime to perform cyber-attacks directed to healthcare organisations causing great chaos and compromising the lives of people, reaching to a point when a doctor is submitted to superlative amounts of stress because it is their responsibility to make life-or-death decisions when systems are disrupted during a delicate process such as a surgery. This can compromise forever the condition of a patient. Cyber criminals are keen to obtain greater and ambitious financial gain regardless of the organisation,

prestige and security posture they are likely adopting or have in place. Criminals understand that money nowadays is in healthcare and they would do whatever it takes to obtain the desired money, even if that implies to extort people. Attacks suffered such as WannaCry ransomware to England NHS in 2017, or the hacktivist group Orangeworm performing cyber espionage through healthcare systems (i.e., x-ray machines) demonstrate that healthcare organisations must address their budgets to cyber security solutions including awareness training in order to protect information trusted by patients and their partners. EHRs possess basically all the life history from a person and if this ends up in the hands of criminals it may possibly imply blackmailing for a lifetime, destroying the reputation of a compromised person or in worst scenarios, planned terrorist attacks attempted against the life of the victim. Cyber-attacks to healthcare are increasing and the level of extortion caused to people is growing as well, therefore the high demand of security professionals and preparation of future generations to protect data in this interconnected world needs to keep up with this growth. Organised crime is taking advantage of selling health records in the dark web considering the wealth of information available, including the history of the person, leading to social engineering attacks without scope (Illmer 2018). The dark web is known for not presenting boundaries or controls but for making the best place for organised crime to work at free will. Even though it is possible to access it through The Onion Router (TOR), attackers are using this network to remain anonymous when attacking the organisation due to its strong mechanisms to remain hidden throughout the internet, making it difficult to investigators to trace them back. However, TOR presents vulnerabilities and attackers are looking at other ways to assure anonymity, considering other options such as blockchain technologies along with other tools such as Virtual Private Networks (VPN) and Proxy routing. In addition, blockchain is currently very popular and attackers are inserting malware into highly sophisticated computers to perform cryptomining due to the benefits of solving as many math puzzles as possible to be considered as the main node between peers.

This chapter analyses the value of healthcare records in the black market, detailing the parameters it presents and why it attracts so much to cyber criminals to steal it along with the future extortion that can cause issues for either organisations and people in general. Moreover, it explains how cyber criminals are taking advantage of the dark net in order to get higher financial gain. This is because the dark web is used not just to sell stolen information, it allows to connect between malicious hackers, trade information about potential targets and limitless applications beyond our imagination. The rest is divided as it follows: Sect. 5.2 explains the value of EHRs for the black market, Sect. 5.3 explains the usage of EHRs for clinical trials and research, Sect. 5.4 details the most common cyber extortion attacks and its impact to the healthcare. Sect. 5.5 analyses blockchain, along with TOR and other common tools used to accomplish anonymity. Finally, Sect. 5.6 concludes this chapter with some further research suggestions.

5.2 Electronic Health Records and Their Value to the Black Market: A Rare Commodity to the Organised Cyber Crime

Healthcare organisations are facing a digitalisation era where their main assets such as health records from patients, machines used for medical purposes are being connected to the internet. The deployment of electronic personal health record (ePHR) systems is providing health consumers greater accessibility and a better control over their information. It consists on the migration from medical provider-centred to patient-centred, which if this system is associated with the recently implemented European GDPR (Ducato 2016), provides users a better control of their personal identifiable information (PII). Unfortunately, current healthcare providers are struggling to implement appropriate security solutions to protect their assets due to business digitalisation, and often rely on hardcopy medical records. Therefore, these organisations must identify as soon as possible and determine suitable security controls to reduce impact given by security breaches compromising the information from patients.

Electronic health records (EHR) are offering greater benefits and a significant productivity increase, compared to traditional paper-based systems, and which 83% of regular hospitals are adopting these solutions. Likewise, 96% of hospitals providing critical and customised services are acquiring these systems focusing on the benefit of their patients. However, the digitalisation of these organisations is one of the inefficiencies according to Forbes (Yao 2018) and therefore, EHRs are more susceptible to hacking and theft. Likewise, that other information such as credit cards, bank details, etc., have attracted attackers for its theft, the question now is how much are patient lives worth to hackers?

Hackers are using more sophisticated methodologies in order to insert malicious software into machines for information theft, unauthorized disclosure and extort their victims to acquire financial incomings (Casteel 2018). For instance, the ransomware attack that caused damage to England NHS produced costs of almost £92 million. As shown in the research from Catarinucci et al. (2015) and Rushanan et al. (2014), the processing of Personal Health Information (PHI) tends to be collected in real-time with telemedicine devices connected to IoT networks (i.e. Wearable Body Area Networks WBAN, wireless sensor networks WSN, biotelemetry systems), easing the procedures from General Practitioners (GPs), making fast decisions, and avoiding unnecessary appointments with patients.

In 2017 Deloitte, one of the nominated "big four" organisations, has claimed four large technological innovations that could lead to the speculated hospital of the future. The mentioned technologies are the following (also see Fig. 5.1):

- Usage of blockchain networks to accomplish data privacy and anonymity. It is supposed to offer information only for patients and the capable personnel involved in a certain medical procedure.
- Virtual reality technologies, especially aimed to orthopaedic rehab procedures, making it easier and friendly to patients who are getting recovered from complex and sensitive surgeries that compromised the mobility and motor of his/her body

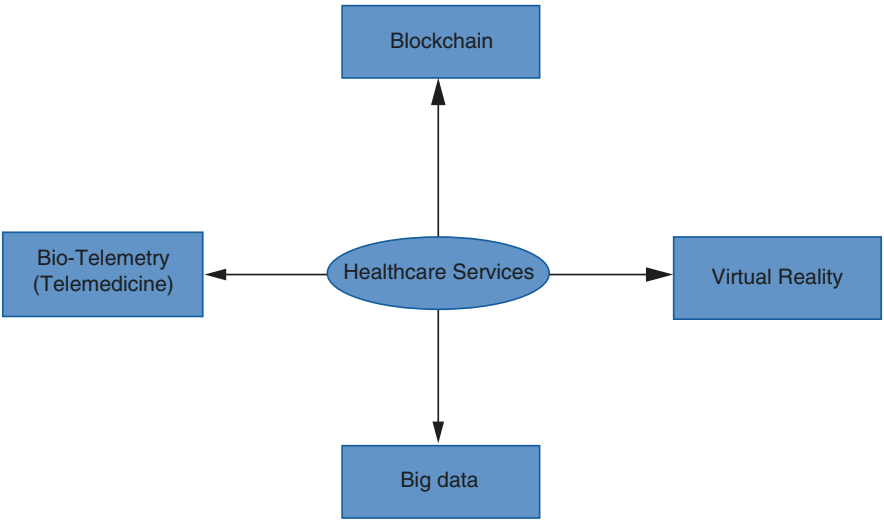

Fig. 5.1 Four innovative technologies for the hospital of the future

(e.g., microdiscectomy performed on the spine given by a herniated disc), experiencing memorable situations and motivating the patient.
- Usage of data science for higher data processing, aimed to medicine and treatment prescriptions at faster responses.
- Bio-telemetry systems, used for patients who require to be monitored in real-time, even when the doctor is not present.

The increased demand on the Internet of Things (IoT), along with cloud computing systems allowed organisations to offer services to users to monitor in real time their health in order to make faster decisions and improve their lifestyle (Islam et al. 2015). The more information users are storing on customised services, the more exposure they are providing to their PII, attracting hackers to exploit other footprinting sources to achieve the data thefts they are looking for (Mendelson 2017). In addition, IoT-based devices and applications are being criticised for not showing the process of data collection and processing. Furthermore, in most of the cases, it does not contain the correspondent consent from its users. Moreover, it is predicted to grow to an estimated amount of 163.2 billion IoT devices within health purposes, highlighting the challenge of data collection through IoT devices without the user being aware of potential issues or threats, (Whitmore et al. 2015), leading to questions such as: Is the data collected disclosed to authorized users as the provider claims? Is the data being used for the only intended purposes? (O'Connor et al. 2017)

In addition to IoT, cloud services are providing a significant support to healthcare organisations (Shu and Jahankhani 2017) as per Fig. 5.2 and it provides structure in the following:

- Higher savings on data storage because of the availability of hiring Software as a Service (SaaS) cloud systems.

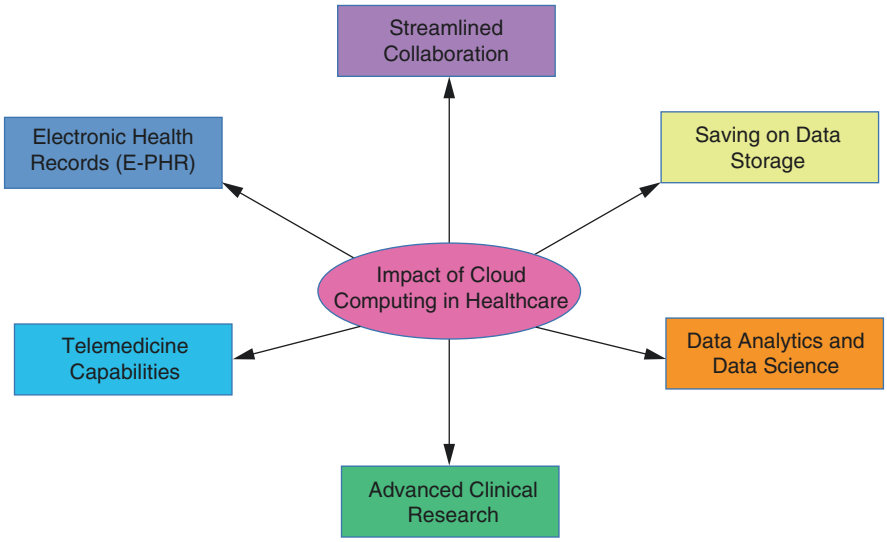

Fig. 5.2 Impact of cloud computing on healthcare

- Data science used to process and analyse millions of data processed throughout the network.
- Advanced clinical research, used for clinical trials, where results are stored from tests, behaviour of new medicines tested on patients including secondary effects of medicines and measures suggested to enhance capabilities of new medicines and treatments.
- Telemedicine capabilities, thanks to the usage of wearable devices, Wearable Body Area Networks (WBAN) and Machine to Machine (M2M) communications for complex procedures applied in modern medicine.
- Streamlined collaboration
- Electronic Health Records in order to manage them, along with the healthcare systems being used.

EHRs offer a significant wealth of information, attracting hackers to exploit and steal. It contains information such as:

- Demographic information.
- Full names, which are the same as encountered on personal IDs, driver licenses, passports.
- Address history, including places where the patient lived before.
- Work history, including former work places where the patient provided services to previous organisations.
- Names, ages, contact details from relatives, which can belong to parents, siblings, life partners or any representative the patient trusts. The health provider contacts this person in case the patient faces an emergency.
- Financial information, including bank details, credit/debit cards.

- Social Security Number (National Insurance Number in the UK)
- Medical history, which contains sensitive information. It includes details of previous medical appointments along with details from doctors and nurses. Moreover, it has critical information such as allergy details, surgeries the patient was submitted, results from medical diagnosis such as x-rays, electromagnetic resonance, etc. The appointments listed include diagnosis, prescriptions, treatments and dates for the next medical control organised in a chronological manner.

As shown beyond just data, EHRs contains precise details of the victim's life. Once a health provider is subjected to a security breach compromising patient records, customers who suffered from the breach can likely get exposed to extortion by way of blackmail that can continue for a considerable time or even a lifetime. Furthermore, if EHRs contain additional information such as cancer diagnoses, sexually transmitted diseases, psychological conditions established (i.e., asperger syndrome, autism, depression, alcoholic), the victim can be exposed to public embarrassment or political assassination depending on the goals of hackers.

One of the greatest challenges that has overshadowed the web's benefit is the risk associated to our data privacy, security and rights. This is now becoming such an issue that the founder of the web Sir Berners-Lee (Sky News 2018) through the world wide web foundation and the recent web summit in Lisbon has launched the charter for the web: a Magna Carta of digital rights. Speaking from the Web Summit, Berners-Lee said: *"The web is at a crucial point. More than half the world's population remains offline, and the rate of new people getting connected is slowing. Those of us who are online are seeing our rights and freedoms threatened. We need a new Contract for the Web, with clear and tough responsibilities for those who have the power to make it better. I hope more people will join us to build the web we want."*

The report, "The Case for the Web", as part of web foundation campaign, has outlined the key action needed to confront risks on data privacy and more importantly the centralisation of power online among a small group of companies. The report highlights that living in the connected world with billions of people in countries where there is no comprehensive law on personal data protection, would particularly leave societies vulnerable to increasingly common incidents involving breaches of personal data. This is ever more important when dealing with Health.

The ordeal for a patient in discovering that their identity is available for criminals to gain benefit from, because of the healthcare institution having been breached by a malicious attacker, is extremely concerning. The large scale WannaCry ransomware attack of 2017 highlights the dangers of large scale data breach which no one really knows how far and wide the identity theft will appear or manifest itself. On the deep web, the value of the medical data is said to be ten times that of stolen credit card numbers, (Francis 2018) and if big data sets are available they can go for large sums of money. So, the attraction to attack the healthcare industry is clearly one motivated by its value on the deep web. There likely is a much larger adverse effect from those that suffered from identity theft and the criminal victimisation because of the data breach and a deep violation of the patient's privacy (Stofko 2018). The loss of data surrounding identity is of course a problem but so too can be sensitive medical history and therefore the impact is far deeper and greater than losing credit card

details. Well, at least with GDPR in place data breach notification must be announced within 72 h or penalty consequences will be delivered. Consequences are worse, as unlike a stolen credit card which can be cancelled and therefore if discovered in time by the victim they can at least deploy damage limitation strategies (Shu and Jahankhani 2017). But medical records hold valuable data points that map a person's identity and can't be changed and give the attacker time to work out how to plan the best outcome from stolen data.

Various quantitative and qualitative analysis research demonstrate a few reasons for healthcare to consider alternative mechanisms such as blockchain (Paterson 2018). Whilst blockchain is a technical tool to aid and support a better method than currently deployed, the driving forces are enhancing privacy of data and securing a better transparency of data that ultimately should help achieve towards the goal of protecting the patient. One can argue in favour of blockchain if just a single aspect can show the benefits such as interoperability.

After some research done on the dark web site WallStreet Market (see Fig. 5.3), at the left of the picture, cards are worth between $15 and $22, while at the right side it is seen that social security numbers are worth $3. However, considering the details that EHRs have, it could be worth hundreds, or thousands of dollars given by all the details they present and the unlimited scope of malicious actions that attackers can perform, derived by accessing this information.

Looking back in 2015 (Seleman 2018), past security breaches to health providers compromised the information of 100 million personal health records (PHRs), and it involved the investment of millions of dollars to remediate their systems. In addition, healthcare organisations heavily regulated themselves had to afford the payment of penalties of $380 per PHR stolen. In 2016, it was reported 450 security breaches from health providers compromising 27 million of PHRs, which over 65% of the notified incidents were given by insider threats. In 2017, Marsh-Microsoft Cyber Perception elaborated a survey between July and August and from their results, 27% belonged to healthcare organisations who were victims of cyber-attacks in the past 12 months, which was more than financial institutions (20%), and almost twice compared to Information and Communication Technology industries (14%).

Over the last years, the impact from cyberattacks has overcome boundaries and no region in the world is completely immune to incidents in the cyber space. As seen in the information above, human lives are critical as well as its sensitive information it holds, making the healthcare market the perfect target for organised cybercrime. Ransomware attacks such as WannaCry and NotPetya had an extended scope affecting the health and insurance service. Another aspect of great concern are places which have poor security maturity and may take from five to ten times longer to detect an intrusion compared to global counterparts. Cybercrime organisations should be viewed in many ways as other kinds of organised crime or businesses, and there they run the operational structure in a similar way; where there are those in charge giving orders, but instead of traditional personnel, they utilise knowledge from their geeks they employed and highly specialised experts who look for and exploit vulnerabilities in the code of commonly used programs (Yip et al. 2017). Therefore, cybercrime is a global industry and is becoming a big business in the dark web. Figure 5.4 shows a snapshot of recent attacks in the healthcare industry,

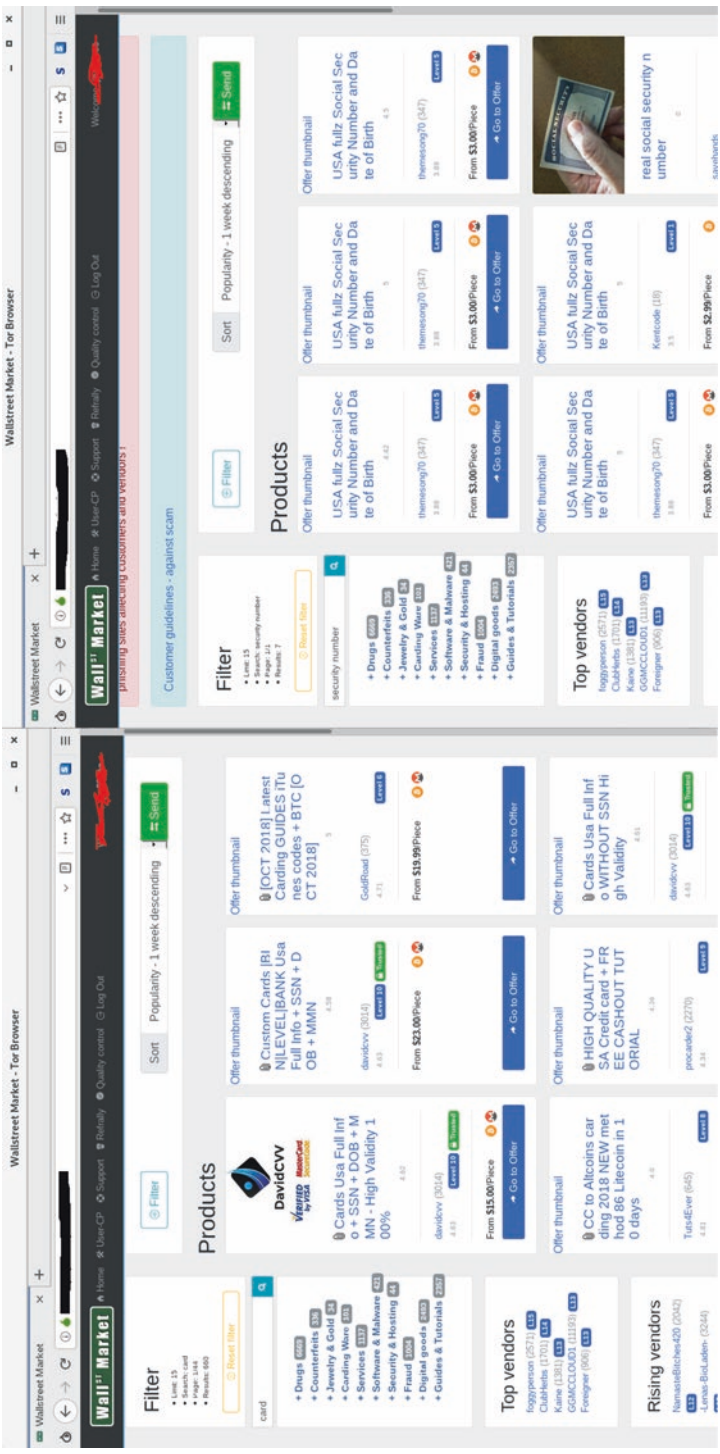

Fig. 5.3 Prices of credit cards (left) and social security numbers (right) at Wall Street Market Darknet Site

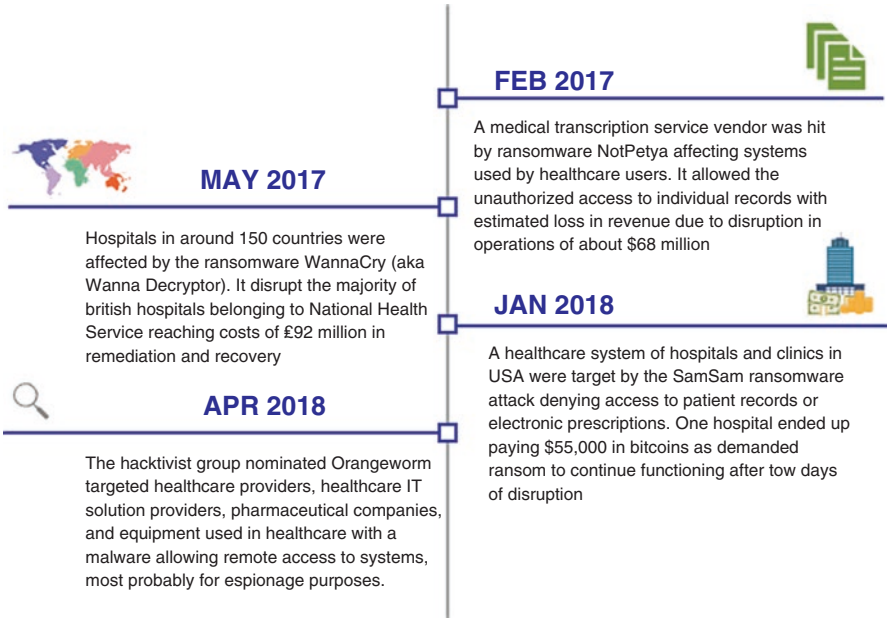

Fig. 5.4 Time line of latest extortion-based cyber attacks to healthcare sector

such as in January of 2018 with the injection of the SamSam ransomware, or in April a hacktivist group named Orangeworm remotely accessed equipment and systems for possible espionage purposes (Wyman 2018).

Criminals use cryptocurrency for various reasons. The main ones are because of the anonymity it offers and also for the purpose of avoiding the payment of taxes at their respective countries requirements and rates, especially within the EMEA region. In addition, along with cryptocurrency incoming, cyber criminals are developing malware to execute cryptomining on the background of infected hosts. Considering that next the generation of healthcare providers will use technologies such as blockchain for data privacy, virtual reality, internet of things connecting dedicated machinery to private networks increasing productivity and supporting on delicate procedures such as surgeries, and data science for the processing of higher amounts of traffic, then it demands the purchasing of sophisticated computers. Assets in the healthcare market are showing higher value and attackers are looking for new tactics and methods in order to accomplish their malicious goals creating extortion on organisations, taking advantage of the fact that shutting down systems within hospitals and clinics creates high pressure on employees, doctors, etc., because they have to make life-or-death decisions.

Cybercrime does not present boundaries, and they are always keen to find new skilled people in order to join their cause. Over the last years, it has been appreciated how social media is ruling on time consumption for end users, allowing them to build contact networks, connect with other people and share stories by uploading pictures, sharing files and trading information. Nowadays, social media is being

commonly used within businesses and healthcare organisations and so are not the exception. On the other side, the usage of these platforms allows attackers to steal information and the trading of compromised data. It takes just some minutes to create fake profiles to avoid detection of unusual behaviour under these infrastructures, using it as cybernetic campaigns to attract people in order to join for their cause (Leukfeldt et al. 2016). Hacktivists groups tend to upload confidential information threatening the integrity and reputation of organisations causing damage and extorting their internal employees. In some countries, included the UK, the healthcare sector is considered as Critical National Infrastructure (CNI), along with vital services such as electricity, water and transportation, making it an attractive target for malicious hackers with great desire of generating chaos. In addition, the business of cybercrime allows to share information between members regarding potential targets using social media and websites allocated within the dark net. It is possible to find reports and journals mentioning how businesses are investing in network and endpoint security in the majority of companies rather than training people to avoid and to respond to a cyber-attack executed by criminals. In fact, besides using social media to elaborate the proper reconnaissance addressed to the potential target, it can be used for scamming, searching exposed personal data belonging to careless people.

Organisations are facing a daily battle within the cyber space, where businesses are defending their assets to protect data trusted by customers. Meanwhile, cybercrime is developing new methodologies in order to steal this information regardless of their motivation. The healthcare industry is facing an era where technology is providing a great contribution to deliver cutting-edge solutions regarding medical treatment, providing a better lifestyle for patients. Therefore, it is important for this market to understand the value of their physical and digital assets in order to apply the most optimal security measures and reduce the risk impact given from organised crime.

Cyber criminals are relying on the growth that the dark web is presenting because of the lack of control, which governments have been struggling to shut down these illegal websites for years. In fact, 4% of the entire internet is the World Wide Web (WWW) commonly known by all end users. Meanwhile, the rest is known as the deep web while a part of this belongs to the dark net, which cannot be found with traditional search engines such as Google. Besides, the dark net offers strong layers of anonymity allowing attackers to be untraceable. The dark web in only accessible using dedicated software that could be either The Onion Router (TOR) or Invisible Internet Project (I^2P). All web pages encountered on the dark net are not controlled by law enforcement therefore, cyber criminals are performing unscrupulous actions taking advantage that users take the risk and navigate through the dark net in order to purchase items which can be currently forbidden to be prescribed.

As seen, cyber criminals are taking great advantage of the lack of governance and control over the dark net, letting them exploit and sell the information stolen on healthcare organisations, medicines that are not legally commercialised on common pharmacies. EHRs from patients can be found on the cyber black market at higher prices and can contain information that cannot be found on other organisations. This is because, users trust their data to these organisations considering the fact that

healthcare services are free in most of countries and in wealthy and highly developed countries they count with highly sophisticated equipment at their disposal.

5.3 Electronic Health Records for Clinical Trials and Research

In healthcare, the development of medicines takes time in order to be finally elaborated and authorized by international committees to be prescribed by doctors. It follows a complex process called clinical trial, which consists in the development, testing, follow-up, improvement and distribution of medicines addressed to human patients. Before starting the process, the trials must be performed with animals and recruits groups of people to evaluate the behaviour of their immune systems, looking for secondary effects of medicines developed. In addition, all this information is recorded in patients' health records and research databases, where attackers find it attractive as well. This is because, they can take competitive advantage to sell in the black market these medicines until they get officially authorized by medical federations for its commercial aspects (Ctu.mrc.ac.uk. 2018). Medical treatment and medicine prescription has been involved in debate for years, specifically pointing out that the consumption of drugs can provide a great improvement on lifestyle; however, because of the way drugs have been processed, distributed and consumed by people, it created a great controversy and medical federations made the decision to forbid the drug consumption. In some countries, it is allowed the consumption of drugs, for example a few months ago Uruguay declared as legal to consume marijuana and once the law has been implemented, it went out of stock immediately in just 2 days in what was expected to last for a month.

Clinical trials are divided in the main phases which are detailed below (nhs.uk. 2018):

- **Phase I** is aimed to measure the safety of new treatments. It assesses the side effects of the treatment, and it involves small groups of people, which are commonly in healthy conditions. For instance, it is examined whether the treatment makes changes on patient such as blood pressure raised, causing any sickness, etc.
- **Phase II** is applied to greater groups of people. It is addressed for patients who are under the required symptoms for which the treatment is being aimed. Researchers analyse whether the submitted treatment is safe and the effects under the required condition.
- **Phase III** involves even greater number of people who are selected randomly to receive the treatment in order to analyse the behaviour of the new treatment. This phase takes longer compared to Phase I and II because the treatment has a different reaction on every patient.
- **Phase IV** is performed once the medicine has been approved by regulatory authorities. It carries out the information of the medicine's effect on people from different countries, ethnicities and evaluates side effects of the medicine related to long term usage.

Clinical trials and research can receive volunteer people, and some clinics hire people in order to test the effects and effectiveness of the new treatment deployed. However, it demands an extended amount of time to analyse the behaviour of the treatment in people. In addition, this process is supposed to be transparent for patients, meaning that only researchers have the knowledge of all the patients submitted to clinical trials, while patients are not aware whether anyone has volunteered to try the effects of the medicine (Weng et al. 2014). One of the great benefits of clinical trials is that patients involved in this process are the first ones experimenting the effectiveness of the treatment, which offers higher possibilities of enhancing their lifestyle before it becomes available for the general public. A negative consequence is when the patient, by accident, uncovers that they are allergic to one of the components of the medicine, making researchers immediately suspend the trial with the person and review the group.

The main outcomes of the results obtained from clinical trials are to prevent illnesses testing vaccines, detect or diagnose illnesses, perform blood tests on patients, treat illnesses by testing existing or new medicines, and analyse psychological support and help people to control their symptoms (De Moor et al. 2015). All this information is allocated under their health records which are managed by the information systems implemented in hospitals and clinics. Cyber criminals are keen to gain access to this information in order to develop their medicines and sell it on the black market before it becomes available to the public or in the worst case scenario, the treatment and its commercialisation gets rejected by authorities (O'Flaherty 2018). Furthermore, having gained this sensitive information allows the black market the opportunity to hire those that don't object to being involved with criminals and perform terrorist acts. For instance, a patient who possess diabetes, who has enemies, can be murdered just by providing him the wrong order in a restaurant causing an immediate heart attack or effects of that intent.

As seen, the ePHR robbery has increased in popularity within the organised crime and the dark net because it leads to numerous social engineering attacks that can extort victims, get financial gain from them along with healthcare organisations involved or in the worst case scenario to perform a terrorist attack, compromising the life of a victim(s). The dark web is the home for cyber criminals and they are keen to get this information in order to plan future attacks. The number of acts that can be performed getting this information is limitless and it can likely be achieved for long term extortion purposes.

5.4 Crypto-Viral Extortion Attacks and Its Impact on Healthcare

Healthcare organisations are prone to three kinds of cyber-attacks that can cause huge amounts of extortion to their employees because of the fact that disrupting systems or compromising the security of their patients leads them to make crucial decisions that compromise their health. The cyber-attacks mentioned are:

- **Denial of Service/Distributed Denial of Service (DoS/DDoS)** – Consists in the degradation of the performance from computer systems and machinery used in healthcare, which are connected within a corporate network. Currently there are machines connected to computers which insert the information and allocate it along with EHR from patients accelerating the process of the organisation. This attack can also disrupt completely the functionality of computers and hosts within the network, and there are artefacts performing processes such as x-ray, magnetic resonance, fridges to maintain blood texture, health monitoring devices including the personal wearable, (Snell 2018). The distributed attack is done useing botnets, a network of infected computers allowing attackers to flood target computers with huge amounts of traffic, saturating resources from the target such as CPU, RAM memory, stack memory on network devices. For instance, stopping the functionality of a monitoring device while performing a surgery, can cause high stress/pressure on doctors because they could likely struggle on the next steps due to the exposure the patient is being submitted to and cause irreversible damage or disease; therefore the decisions made by doctors during delicate processes are extremely crucial.
- **Ransomware –** This attack has seen a significant increase in popularity for the benefits attackers are receiving from injecting this malicious software in healthcare organisations. This malware can either lock the access to computer systems or encrypt critical files within hosts. In other words, attacks are kidnapping data processing systems or devices and the only way users can retrieve their systems back is by paying the demanded ransom. Some victims of ransomware did not pay the demanded amount of money because they strongly believed that although the payment is sent it does not guarantee attackers will reset systems to their last version. The best countermeasure at the moment to remediate this cyber-attack is the availability of backup systems in off-line sites because ransomware has gotten more sophisticated and are looking to destroy backup servers to assure victims pay the demanded ransom and obtain financial incomings for this cyber extortion technique.
- **Information Theft –** Cyber criminals are always looking for new information that organisations provide, and nowadays healthcare providers are storing plenty of valuable information, which is increasing steadily in the black market. Healthcare organisations are the ones in the market who possess tons of sensitive information and being stolen by attackers causes damage to the reputation of the organisation; but it also exposes patients to potential harm. As analysed beyond, unauthorized access to personal data leads to cyber criminal to perform further limitless cyber-attacks with all the gathered information. It can be something as simple as blackmailing patients for a lifetime, or something more harmful such as identity theft given by selling this information in the black market. The scope for damaging people and organisations thanks to data theft is absolutely limitless.

Analysing the mentioned threats from an organisational standpoint, All roles within healthcare services have an important impact in terms of protecting sensitive data, which is trusted by patients and doctors as well. It is likely that its IT infrastructure is not well safeguarded due to a limited budget. Nevertheless, personnel

must count with suitable training not just for the accomplishment of the goals of the organisation. It also has to be done in order to apply suitable preventive cybersecurity measurements to protect the information and prevent incidents that could stop medicine procedures, this is because there is the possibility that an incident of high magnitude can cause irreversible damage.

In addition, to strengthen the anonymity of criminals, they are abusing the usage of cryptocurrency, with special mention to Bitcoin, a blockchain technology that provides anonymity and because this system is based on trust and does not have a centralized authority, it is speculated as uncontrolled as well. The next section will describe how cyber criminals take advantage of tools such as TOR and blockchain technologies to accomplish anonymity during the execution of cyber-attacks.

5.5 Analysis of Blockchain Technologies, the Onion Router, and Other Tools Used for Anonymity During the Execution of a Cyber Attack

(a) Blockchain

Blockchain is a very intriguing new technology that started gaining popularity for cryptomining purposes. With the increased rate in cryptocurrencies such as Bitcoin, Ethereum, etc., people started to do research about how the business works and the benefits of doing cryptomining. It promises great enhanced features in terms of security and data privacy that could transform not only the FinTech market, but other industries too. Other sectors such as Retail, E-commerce, Internet of Things, Smart Energy and Healthcare are investing deeply in research and deployment of applications adopting the optimised usage of blockchain technologies.

Blockchain is a distributed system, secure, peer-to-peer (P2P) environment that works on the principle of trust, sharing and the mutual calculation of transactions. In addition, if is a fault tolerant system, does not count with a centralised application managing the network. Moreover, following Fig. 5.3 it has strong cryptographic algorithms, using block-based cryptography. Every transaction is submitted to a hashing procedure, normally SHA-256 for Bitcoin transactions. There are cryptographic schemes, exactly Elliptical Curve Digital Signature Algorithm (ECDSA), used to sign a hash digest from the previous block (N-1). This digest is used to calculate the hash digest of the current block (N). In addition, each block contains the Merkle tree root hash to keep the information of all transactions executed in the network. In the blockchain network, each header contains a nonce, timestamp, value of previous hashes done, gas limit, the difficulty along with other parameters including meta-data making difference between the different existent blockchains (see Fig. 5.5).

To achieve the trust between peers, it uses several mathematical algorithms, depending on the type of blockchain. This technology offers security and transpar-

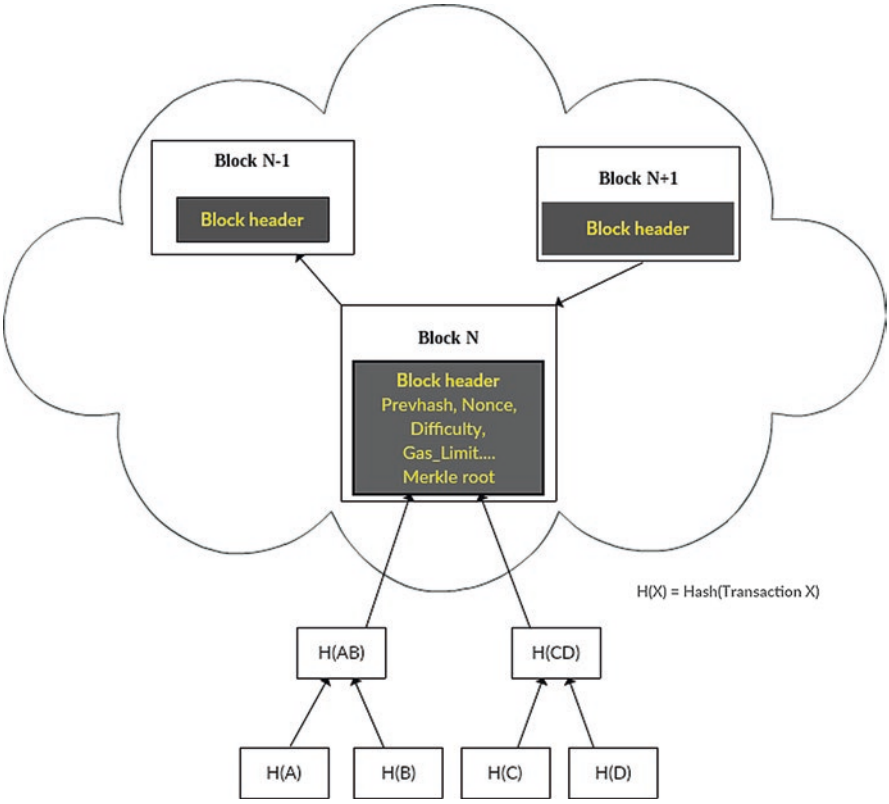

Fig. 5.5 Blockchain structure

ency of transactions, privacy, availability, immutability; however, because it does not have a central authority; this P2P network can be speculated as uncontrolled.

The most popular blockchain technologies used for cryptomining are Bitcoin, Ethereum, Monero and a commercial-based one named Hyperledger, developed firstly by the Linux Foundation developing the partnership between industries by advancing blockchains. Hyperledger received the contribution of great companies such as IBM, Monax, Soramitsu and Intel. One of the newest features hyperledger presents is that peers are divided into two separated runtimes with three different roles: endorser, committer and consenter, offering independent scalability.

As seen, lots of organisations are keen to create services and enhance their current portfolios using the blockchain as an innovative solution and on the other hand, the huge amounts of data being processed throughout the network and thus, polluted payloads or data misuse are great concerns that require some actions to resolve. The TOR network leveraged the blockchain to assess some unusual behaviours. For instance, the blockchain can be used by cyber criminals to deliver malware by inserting malicious payloads to deploy encryption using public key cryptography and selling the private key to decrypt the content and abuse this technology feature. In

addition, blockchain can be exploited to deliver malicious payloads to users dedicated to cryptomining such as ransomware. And nowadays, cryptomalware has increased in popularity inserting malicious payloads into systems used for cryptomining, abusing the resources of computers especially in bitcoin systems, because of its functionality. Computers with mining applications are solving as much mathematical puzzles as possible consuming the CPU and GPU if computers count with graphics card. This is called in Bitcoin, Proof-of-Work (PoW). It requires 51% of all the math puzzles solved for the peer to get control of the node and therefore, better rewards for the connected peer. Cryptomalware is used to create botnets and perform mining at the background abusing the resources of the infected user and supporting cyber criminals to solve more puzzles, take control of the node and get higher rewards. Great potential targets prone to cryptomalware attacks are gaming computers, supercomputers, highly sophisticated servers, in healthcare equipment and devices connected to networks used for medical purposes (Moubarak 2017). In addition, a great concern of blockchain networks will mostly lead to several ways of mechanisms behaving in an unusual manner because of the potential expansion of blockchain networks that are uncontrolled. Another area of misuse in healthcare systems, is allowing the blockchain network to perform as Command and Control Servers to the infected bots in order to receive additional instructions or malicious payloads.

(b) The Onion Router (TOR)

The Onion Routing (TOR) system, is a common network that assures anonymity for TCP-based applications (web browsing, remote shell, instant messaging), along with stream isolation for location-hidden services. This network consists of approximately 12,000 routers, divided in several layers, which each router has specific roles depending on the level of confidentiality given by the network. TOR is a distributed system that forwards client requests using encryption techniques from the source to the last node before arriving to the server (see Fig. 5.4). Firstly, the TOR clients start looking for its registered nodes on the internet analysing within their databases, which are considered as trusted and redundant authority systems in charge of listing to all the nodes on the TOR network. This system works on a circuit based network which downloads the information of related nodes setting a circuit, which requires a minimum of 3 nodes on the established routing table during the connection between client and server.

Encryption is the main feature to achieve anonymity under this network. Comparing this system with common sites, the WWW nowadays employs encryption protocols such as SSL (Secure Sockets Layer) to protect client data or other content within the packet payload as it traverses throughout the internet. In case of TOR networks, once the connection is established between client and server, each node within the network hides the pair of keys for encryption and decryption respectively. Moreover, each node assigns a different IP address of the server and client allowing complete anonymity during the session built. Hence, every node does not have knowledge about the routing table, they only send/receive the encryption and decryption keys, whilst the client/server send/receive the information in plaintext. Furthermore, to prevent data tampering during the established session from anony-

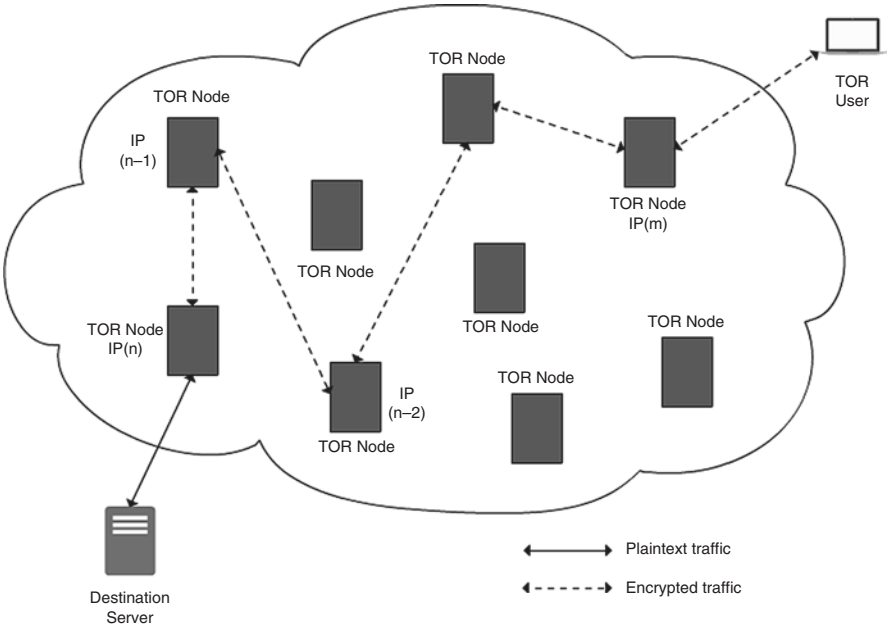

Fig. 5.6 Simplified overview of TOR network

mous clients including eavesdropping, the same process is done for additional requests but using different chain relay nodes. Therefore, each session has a unique circuit built and route within the network (see Fig. 5.6).

Cyber criminals are taking great advantage of the TOR network because a non-negligible part of it is managed in a obscure manner by the TOR foundation. Moreover, most of the bridge router locations are still unknown, and considering the features that this network gives, it makes forensic investigators struggle tracing back the location of these authors who performed cyber-attacks. It is speculated that cyber criminals are under the dark net as refugees of the Internet, taking advantage of freedom and exploiting the benefits of being anonymous while navigating throughout the internet.

(c) Other Common Tools

Even though the TOR network is secure and private, it does not guarantee the expected 100% security, and cyber criminals are aware of this feature. In fact, it is possible to review reported vulnerabilities on the website www.cvedetails.com on the Torproject. For instance, the vulnerability CVE-2017-16,541 reported on 4th of November of 2017 detailed that an unpatched version of TOR below 7.0.9 in devices using MacOS and Linux allows attackers to bypass the anonymity feature and discover the IP address of the client. Considering this feature, cyber criminals are keen to deploy stronger track covering mechanisms, so forensic investigators would

struggle to locate the people and devices involved in an cyber-attack extorting the intended victims.

An extra capability added during a cyber-attack is the configuration of proxy routing services within the machines involved in the cyber-attack. A proxy is a service which acts as a bridge connection between client and server. When the client is sending a request to establish a new session with the server, in the packet the IP address of the proxy server is shown instead of the end user, allowing it to hide their location. In addition, it is possible to change the port during a TCP session between client and server (see Fig. 5.7). A common freeware tool and available on the market is the usage of a packaged nominated **Proxychains**, which allows the attacking host to navigate through the number of proxies configured hiding the IP address of the client. This service is available by default in the penetration testing distribution **Kali Linux**, used commonly by ethical hackers and pen testers. It allows to configure the number of proxies the request must be transmitted through prior to reaching the destination. For instance, if the service is configured with four proxy IP addresses, the packet header will be submitted to a change of sender IP address, four times before reaching the receiver.

In addition to the usage of proxy routing, cyber criminals are always keen to hide the information allocated within the payloads of a transmitted packet. One of the best options is the usage of a Virtual Private Network (VPN), which creates a tunnel during an established session, and all the information navigating throughout it, is submitted to strong encryption techniques. Therefore, joining the usage of proxy routing, a VPN, along with configuring the machine to navigate through TOR network, it would end in a complex network shown in Fig. 5.8.

When performing a cyber-attack, criminals are considering two important factors, how much worth is to perform the specific attack to a particular target, along with time consumption. Even though the configuration of proxies, implementation of VPNs and navigating through TOR means significant delays in the connection established between the attacker and the target, the importance of hiding is vital for

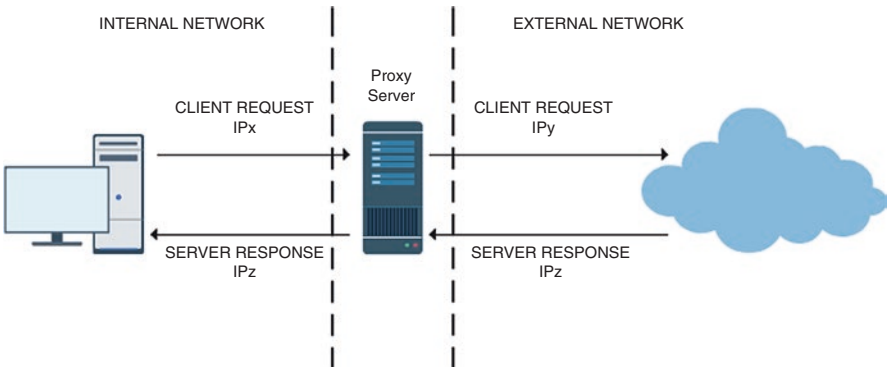

Fig. 5.7 Performance of a proxy to assure anonymity

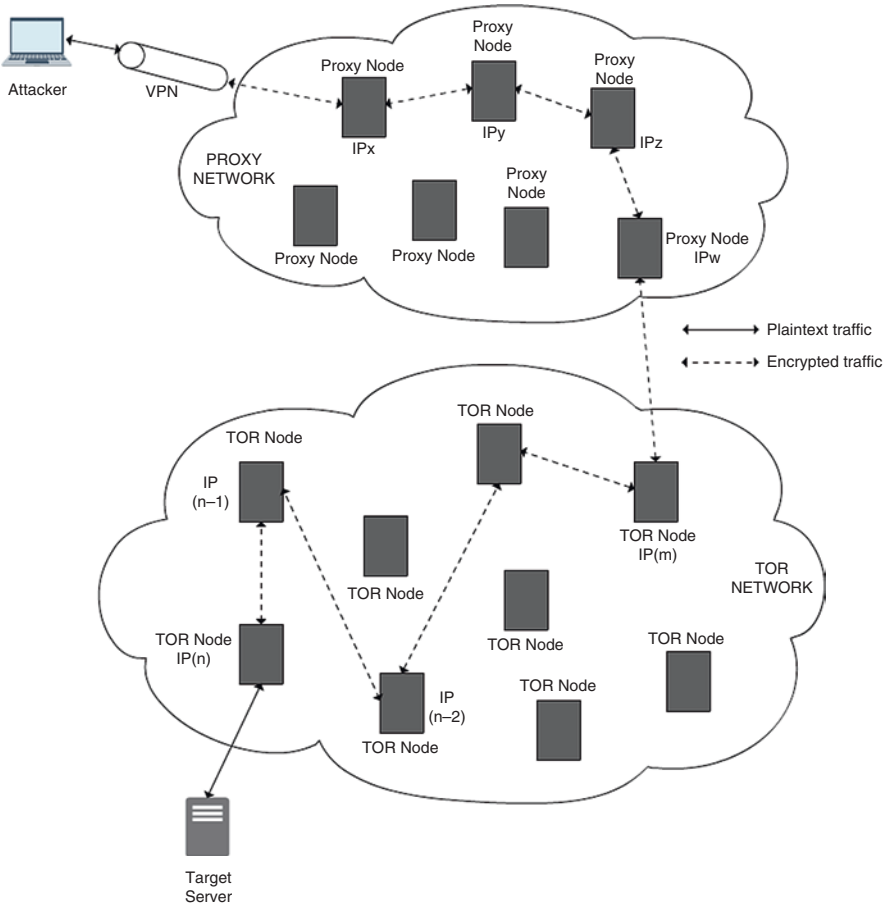

Fig. 5.8 Possible network used by cyber criminals to assure enhanced anonymity during a cyber attack

criminals during an attack to take advantage of the rewards obtained. The delay caused by this pattern can be measured considering the following information:

- Consider the delay caused by encrypting and decrypting the information that is transmitted throughout the VPN
- Delays caused by transmitting packets through different proxies including the delay caused by replacing the IP address
- The delay caused by the usage of TOR network, finding available nodes. Considering that it is required a minimum of 3 nodes as mentioned beyond creating the circuit. In addition, the connection between each node replaces the IP address and includes encryption during the communication.

Even though the session between attacking host(s) and target(s) has been affected by the delays applied due to the features mentioned above, it can take years for

cyber investigators to deter the pattern of the attack, taxonomies followed by hackers and uncover their identities. When tracing back the unauthorized system it is important to follow IP addresses from the sender to find the original location; however, applying the mentioned techniques could likely lead investigators to fall under a limitless mesh that could lead them to abort the investigation.

5.6 Conclusion and Further Research

It has been analysed that cyber criminals are keen to accomplish their purposes no matter what it takes for them to achieve or who can be affected. They are basically financially driven or with the intention to create chaos within organisations, critical infrastructures and with greater chances of generating nation-state alerts. The healthcare sector is totally prone to the most dangerous cyber-attacks because of the information they manage along with the great responsibility of assuring that patients remain alive even when systems get severely disrupted. Even though it is possible to trade stolen information by using social media platforms such as Facebook or Twitter, criminals are keen to keep using the dark web thanks to the limitless scope that an uncontrolled network can provide. In addition, cryptocurrency mining is gaining popularity and criminals are inserting malware into robust machines and stealing resources following the behaviour of a Denial-of-Service (DoS) attack. Likewise, TOR assures anonymity, blockchain offers same features; however, none of them offers 100% anonymity because of vulnerabilities from their systems or the possible extraction of metadata, providing valuable information for forensic investigators. Therefore, despite increasing the time response because of hiding the IP addresses through proxy routing and encrypting data due to VPN, it enhances the anonymity and increases the possibility of remaining hidden when performing a cyber-attack throughout the internet. Although healthcare organisations are spending lots of money in network and endpoint security, it will not stop the organised crime businesses to keep looking for different methods in order to perform data theft or any other malicious activity that could extort from people, to hire skilled people and join their cause. It is important to point out the protection of EHR in health organisations, and the impact of stealing it, enables it to reach to different attack taxonomies, paths, methods and especially diverse social engineering threats due to the sensitivity of the information stolen. For further research it is suggested the application of the anonymity mechanisms, mentioned in this Chapter, be tested in virtual environments to extract precise data of the strength of the security and privacy they claim to assure. In addition, it is recommended to keep navigating through the dark web to discover whether criminals are keen to acquire different assets from organisations to alert the market before suffering a legitimate data breach; the dark net evolves as well as the common internet and it is necessary to keep eye on what cyber criminals are up to. However, it is recommended to take the necessary security measures to ensure privacy while browsing through the dark web. TOR is a good tool to navigate through but to enhance the anonymity hiring a VPN service

and configuring proxies to hide the original IP address is suggested as well because of the flaws that web applications show frequently. Likewise, healthcare organisations must invest in research for strong security mechanisms because of taking responsibility of patients lives and it must be recommended for higher budgets aimed to the cyber security of these organisations and the appropriate measures to ensure confidentiality, integrity and availability of 99.999% system uptime; as expected with implementing ICT infrastructures. With the awakening of cutting-edge technologies supporting enhanced medical treatment, it is required to further investigate in terms of security to ensure business continuity and higher levels of reliability in this interconnected world. People must not get surprised that in other countries around the world that likely they would consider healthcare as part of critical infrastructure, following the example like the UK for instance, and therefore the requirement of regulatory compliance and research on technological areas such as IoT must be addressed to this sector in terms of cyber security.

References

Casteel K (2018) The DOJ wants to stop drug sales on the dark web, but that's a tough task. [online] FiveThirtyEight. Available at: https://fivethirtyeight.com/features/the-doj-wants-to-stop-drug-sales-on-the-dark-web-but-thats-a-tough-task/. Accessed 13 Nov 2018

Catarinucci L, De Donno D, Mainetti L, Palano L, Patrono L, Stefanizzi ML, Tarricone L (2015) An IoT-aware architecture for smart healthcare systems. IEEE Internet Things J 2(6):515–526

Ctu.mrc.ac.uk (2018) What is a clinical trial?. [online] Available at: http://www.ctu.mrc.ac.uk/about_clinical_trials/what_is_a_clinical_trial/. Accessed 22 Nov 2018

De Moor G, Sundgren M, Kalra D, Schmidt A, Dugas M, Claerhout B, Karakoyun T, Ohmann C, Lastic PY, Ammour N, Kush R (2015) Using electronic health records for clinical research: the case of the EHR4CR project. J Biomed Inform 53:162–173

Ducato R (2016) Cloud computing for s-health and the data protection challenge: getting ready for the general data protection regulation. In: Smart cities conference (ISC2), 2016 IEEE International, IEEE, pp 1–4

Francis R (2018) Healthcare records for sale on dark web. [online] CSO Online. Available at: https://www.csoonline.com/article/3189869/data-breach/healthcare-records-for-sale-on-dark-web.html. Accessed 13 Nov 2018

Illmer A (2018) Social media: a cybercrime hunting ground. [online] BBC News. Available at: https://www.bbc.co.uk/news/business-36854285. Accessed 23 Nov 2018

Islam SR, Kwak D, Kabir MH, Hossain M, Kwak KS (2015) The internet of things for health care: a comprehensive survey. IEEE Access 3:678–708

Leukfeldt ER, Kleemans ER, Stol WP (2016) Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks. Br J Criminol 57(3):704–722

Mendelson D (2017) Legal protections for personal health information in the age of big data – a proposal for regulatory framework. Ethics Med Public Health 3(1):37–55

Moubarak J, Filiol E, Chamoun M (2017, October) Comparative analysis of blockchain technologies and TOR network: two faces of the same reality? In: Cyber security in networking conference (CSNet), 2017 1st. IEEE, pp 1–9

nhs.uk (2018) Clinical trials. [online] Available at: https://www.nhs.uk/conditions/clinical-trials/. Accessed 22 Nov 2018

O'Connor Y, Rowan W, Lynch L, Heavin C (2017) Privacy by design: informed consent and internet of things for smart health. Procedia Comput Sci 113:653–658

O'Flaherty K (2018) Why cyber-criminals are attacking healthcare – and how to stop them. [online] Forbes. Available at: https://www.forbes.com/sites/kateoflahertyuk/2018/10/05/why-cyber-criminals-are-attacking-healthcare-and-how-to-stop-them/#167d8e507f69. Accessed 23 Nov 2018

Paterson A (2018) How cybercriminals are using blockchain to their advantage|SecurityWeek.Com. [online] Securityweek.com. Available at: https://www.securityweek.com/how-cyber-criminals-are-using-blockchain-their-advantage. Accessed 13 Nov 2018

Rushanan M, Rubin AD, Kune DF, Swanson CM (2014, May) SoK: security and privacy in implantable medical devices and body area networks. In: Security and privacy (SP), 2014 IEEE symposium on. IEEE, pp 524–539

Seleman M (2018) Ransomware ravages healthcare: cryptoviral extortion in the healthcare sector

Shu IN, Jahankhani H (2017) The impact of the new European General Data Protection Regulation (GDPR) on the information governance toolkit in health and social care with special reference to primary care in England. In: Cybersecurity and cyberforensics conference (CCC), IEEE, pp 31–37

Sky News (2018) Web creator sir Tim Berners-Lee: I see a revolution. Starting right now. [online] Available at: https://news.sky.com/story/web-creator-sir-tim-berners-lee-i-see-a-revolution-starting-right-now-11559034. Accessed 24 Nov 2018

Snell E (2018) How healthcare organizations can reduce cyber extortion risk. [online] HealthITSecurity. Available at: https://healthitsecurity.com/news/how-healthcare-organizations-can-reduce-cyber-extortion-risk. Accessed 13 Nov 2018

Stofko L (2018). How are the deep web and dark web affecting healthcare today? [online] CIO. Available at: https://www.cio.com/article/3228253/internet/how-are-the-deep-web-and-dark-web-affecting-healthcare-today.html. Accessed 13 Nov 2018

Weng C, Li Y, Ryan P, Zhang Y, Liu F, Gao J, Bigger JT, Hripcsak G (2014) A distribution-based method for assessing the differences between clinical trial target populations and patient populations in electronic health records. Appl Clin Inform 5(2):463

Whitmore A, Agarwal A, Da Xu L (2015) The internet of things – a survey of topics and trends. Inf Syst Front 17(2):261–274

Wyman O (2018) [online] Oliverwyman.com. Available at: https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2018/july/holding-healthcare-to-ransom-industry.pdf. Accessed 13 Nov 2018

Yao M (2018) Your electronic medical records could be worth $1000 to hackers. [online] Forbes. Available at: https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#778f241c50cf. Accessed 13 Nov 2018

Yip M, Webber C, Shadbolt N (2017) Trust among cybercriminals? Carding forums, uncertainty and implications for policing. In: Policing cybercrime. Routledge, London, pp 108–131