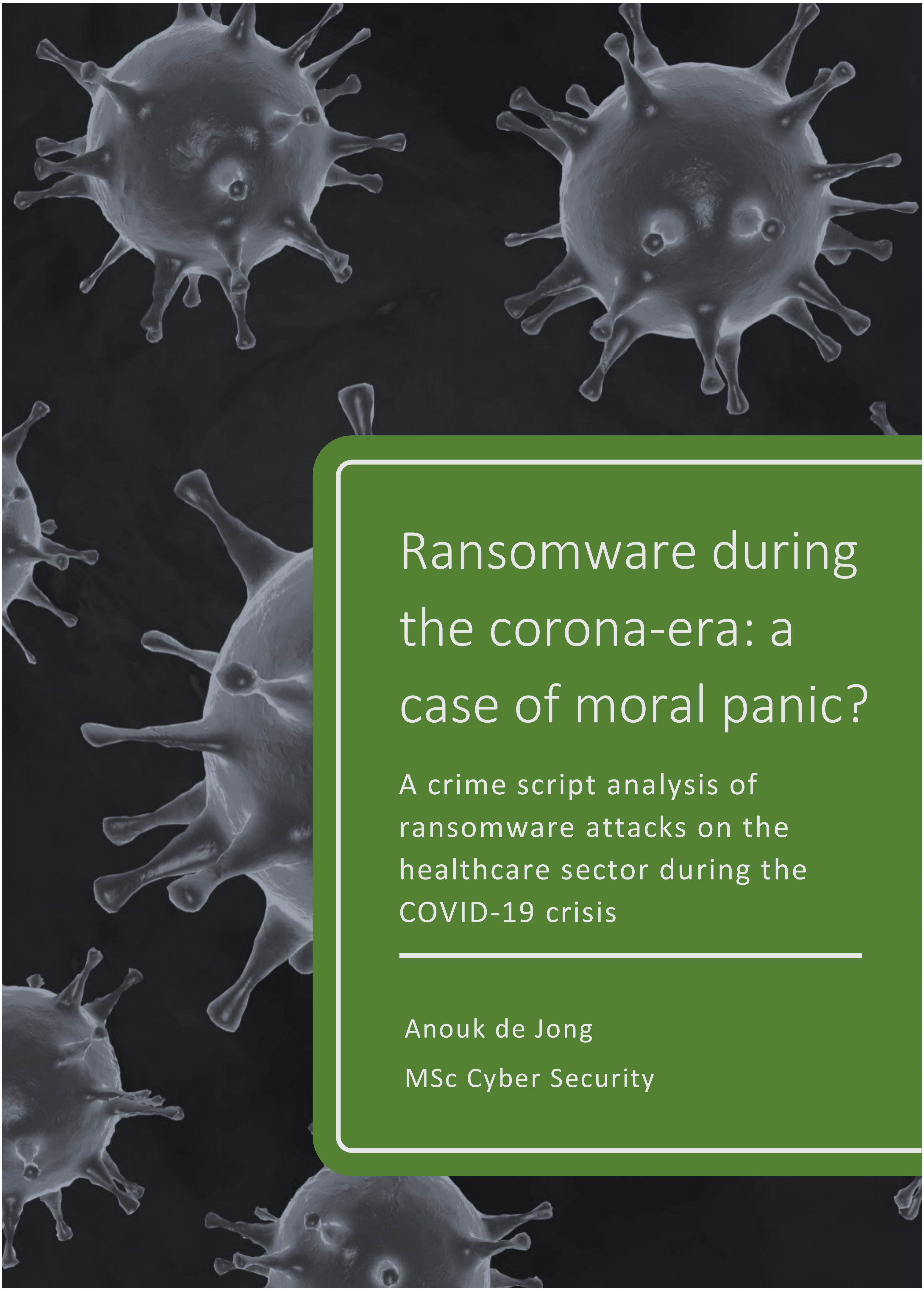


Ransomware during the corona-era: a case of moral panic?

A crime script analysis of ransomware attacks on the healthcare sector during the COVID-19 crisis

Anouk de Jong

MSc Cyber Security

Ransomware during the corona-era: a case of moral panic?

A crime script analysis of ransomware attacks on the healthcare sector during the COVID-19 crisis

By Anouk de Jong
s2419637
a.de.jong.20@umail.leidenuniv.nl

Supervisor: Dr. T. Tropina
Second reader: Dr. R. Leukfeldt

Thesis in fulfilment of the Master in Cyber Security at the Leiden University

07 January 2021

Abstract

Many have expressed their concerns of the increase and severity of ransomware attacks targeting the healthcare sector, in particular hospitals, during the corona-era. A combination of the healthcare sector's reliance on its systems and the often urgent need to access (medical) data means that some cybercriminals have identified the healthcare sector as a suitable target. Some even claimed that the pandemic has cause a change in the modus operandi of offenders deploying ransomware. This qualitative research examines to what extent the COVID-19 pandemic truly changed the modus operandi of offenders who committed a ransomware attack targeting the healthcare sector. More specifically, it investigates how a ransomware attack was carried out at the healthcare sector during the pandemic through conducting a crime script analysis. Subsequently, it investigates whether this differs from the situation before the COVID-19 pandemic. The results of this study indicate that the modus operandi changed just a slightly bit from the situation before the COVID-19 pandemic, but no significant changes were identified. This indicates that we must be critical about most of the claims stating that COVID-19 has caused a serious change in ransomware attacks on the healthcare sector opening up new opportunities to avoid moral panic.

Acknowledgements

First of all, I would like to thank my supervisor dr. Tatiana Tropina for her patience, advice and great support. Also, I would like to thank dr. Rutger Leukfeldt for the inspiration and advice. Thirdly, I would very much like to thank all the participants for their contribution and willingness to talk about this topic. Thank you for your honesty and interesting conversations. Even though some matters are not highlighted in the analysis of this thesis, your insights and expertise helped me to enrich my knowledge and shape this thesis to what it has become.

Table of content

List of abbreviations

AES	Advanced Encryption Standard
C2	Command-and-Control
CENTR	Council of European National Top-Level Domain Registries
CISA	Cybersecurity and Infrastructure Security Agency
COVID-19	Coronavirus Disease 2019
DDoS	Distributed Denial-of-Service
DNS	Domain Name System
FBI	Federal Bureau of Investigation
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICANN	Internet Corporation for Assigned Names and Number
IP	Internet Protocol
IT	Information Technology
MB	Megabyte
NCSC	Nationaal Cyber Security Centrum
PDF	Portable Document Format
RaaS	Ransomware-as-a-Service
RAT	Remote Administration Tool
RDP	Remote Desktop Protocol
RTF	Rich Text Format
RSA	Rivest–Shamir–Adleman
SMB	Server Message Block
URL	Uniform Resource Locator
VPN	Virtual Private Network
WHO	World Health Organization

1. Introduction

“This pandemic brings out the best but unfortunately also the worst in humanity. With a huge number of people teleworking from home, often with outdated security systems, cybercriminals prey on the opportunity to take advantage of this surreal situation and focus even more on cybercriminal activities” (Europol, 2020a, p. 2).

COVID-19 has caused panic around the globe; it is a respiratory illness that can spread from person to person. The virus is a novel coronavirus that was first identified during an investigation into an outbreak in Wuhan, China (NOS, 2020). The coronavirus does not only affect society from a health or an economic perspective, but according to some (Europol, 2020a; Lohrmann, 2020; Politie, 2020) it also has a negative effect on cyberspace. This is also reflected by some news article titles such as: “2020: the year the COVID-19 crisis brought a cyber pandemic” (Lohrmann, 2020), “ransomware surge imperils hospitals as pandemic intensifies” (Lever, 2020), or “COVID-19 pandemic delivers extraordinary array of cyber security challenges” (Grober, 2020).

As a reaction of governments around the globe to control the coronavirus, citizens are advised to work from their homes as much as possible. With many people working from home and using the internet during the pandemic, people’s lifestyle has changed such as by extended teleworking (Limaye, Sauer, Ali, Bernstein, Wahl, Barnhill, & Labrique, 2020) leading to particular cyber security risks. Such risks may arise if employers do not have the required resources to deploy a secure teleworking environment for its employees, especially if the employees’ local network are inappropriately secured (Gregory, 2018). This might unfold opportunities and vulnerabilities to be exploited by cybercriminals. Because more people are spending time online, this would increase the opportunities for cybercriminals to seek for potential victims (Europol, 2020a; Politie, 2020).

Various (inter)governmental institutions, like Europol and the Dutch Police, claim that cybercriminals take advantage of the COVID-19 crisis by adjusting their modus operandi to commit crimes (Europol, 2020a; Politie, 2020). Also, according to Europol (2020a), who has been monitoring the impact of the pandemic on serious and organized crime in the European Union, cybercriminals have adapted their modus operandi to exploit our fears around the COVID-19 pandemic. For example, instead of waiting for the ideal moment to launch the attack, the offenders changed the period between the initial infection with ransomware and the activation of the attack (Europol, 2020a). These reports not only claim that ransomware attacks have become more sophisticated, but also that the COVID-19 pandemic has triggered an increase in cybercrime (Europol, 2020b). Correspondingly, law enforcement authorities across the European Union and United Nations member states claim that there is an increase in cybercrime offences and the nature of cybercrime has gone through a change by becoming more sophisticated (Europol, 2020a; Europol, 2020b; Sabarwal, 2020). On the contrary, in Buchanan's (2017) research about what 'sophistication' in cyberspace actually means, he claimed that the usages of the term 'sophisticated cyberattack' has dramatically grown in use over the last decade. So, how sophisticated are these attacks as claimed by law enforcement authorities and did this actually change over time?

Furthermore, Interpol (2020), Europol (2020a) and the Cybersecurity and Infrastructure Security Agency (hereafter, CISA) (2020), have expressed their concerns by claiming that the most worrying phenomenon during the pandemic is that cybercriminals are targeting the healthcare sector with ransomware attacks, locking healthcare organizations out of their systems in an attempt to extort payments. Cybercriminals especially target those that are at the forefront of dealing with the COVID-19 situation such as hospitals, labs, research organizations and pharmaceutical organizations (Kent, 2020). IT systems are crucial to hospitals as they collect and store sensitive patient data, manage human life support devices and also enable communication for sharing information. Targeting these systems would have far reaching consequences. For instance, it could directly lead to deaths and therefore an even greater panic across the globe might arise during the pandemic (Boddy, Hurst, Mackay & El Rhalibi, 2017). Even though the healthcare sector already experienced ransomware attacks well before the pandemic (Europol, 2020b), Europol claimed that the pandemic caused an increase of the attack surface, with unmanaged IT systems being remotely connected and having access to hospitals' IT infrastructure.

This, taken together with the previously mentioned claims by intergovernmental institutions, raise many questions about to what extent the pandemic exacerbated the problem and brought anything new? Especially because we have seen this happening before in crises such as during the Ebola crisis and the Economic crisis of 2008. During the Ebola crisis cybercriminals have sent emails, pretended to be sent by the World Health Organization (hereafter, WHO), with an attachment that supposed to provide advice on how to stay safe from Ebola. Instead of providing advice via the attachment, it actually contained malware (Dredge, 2014).

Not only health crises, but also other circumstances create opportunities for cybercriminals to commit crimes such as the Olympic Games, the Brexit and the 2019/2020 Australian bush fires (Mahadevan, 2020). Concisely, these are all international crises that give rise to cybercriminals to potentially adapt their modus operandi to misuse the circumstances to their advantage. Cybercriminals are preying on fear and uncertainty by taking advantage of the fact that people are often easily fooled and distracted during times of difficulties. As such, opportunities to attack are on the rise during such crises (McAfee, n.d.; Jackson, 2005; Greenberg, 2008; Guerra, 2009; Thornton, 2009; Tuluc, 2011). Thus, cybercriminals are resolute to take every opportunity to commit a crime and this might indicate that the COVID-19 crisis is no difference.

It is, correspondingly, important to have a critical glance at those reports stating that there is an increase in COVID-19 related cybercrime. Is there truly an increase or is this a typical case of moral panic? Commonsensically, if crime follows opportunities, displacement could take place, this could be in the form of types of crimes, places or targets. Nevertheless, such statements from public institutes have a practical significance. As summarized by Ashby (2016), over-estimating crime can attract more resources and additional legal powers, which in return can make it easier to attract support from the public, media and politicians. Moral panic and exaggerating in this context can lead to the risk of shifting the delicate balance between security and privacy in both policing and surveillance (Lavorgna, 2018b).

The above-mentioned debates reflect the dynamic nature of cyber threats as cybercriminals will continue to seek for new opportunities in cyberspace also during times of crises. Cybercriminals are aware of the importance of the healthcare sector during the pandemic and are willing to target them to get what they want. The well-known criminological statement "opportunity makes the thief" fits well in this situation and it helps to conceptualize and understand why criminals commit crimes. Cohen (1981), an American criminologist, suggested that since opportunities are constantly changing, academics should look at trend patterns to determine how social change influences opportunity and crime rates at specific points in time. Considering that cybercrime during a crisis is such a trend, we could learn from this to prepare and protect ourselves during a next crisis.

As we already know that cybercriminals will use opportunities to commit crimes, this research firstly investigates how they actually misused these opportunities through a crime script analysis. In doing so, this research will zoom in on the healthcare sector given the importunateness. Not only will knowledge of how criminals operate help us to detect and prevent crime, but it also shines a light on the contextual aspects of cybercrime (Yin, 2003; Nurse, 2018). Thus, by gaining an understanding of how cybercriminals exploit opportunities during the COVID-19 pandemic targeting the healthcare sector, relevant actors such as law enforcement agencies and healthcare institutions can increase their resilience to avoid damage or even deaths.

Secondly, with this knowledge, this research will investigate whether the aforementioned claims regarding the changing nature of ransomware are justified or whether this is a case of moral panic. This will be investigated by analyzing if the pandemic has changed the modus operandi of offenders. By investigating whether this pandemic has actually brought about a change or if it is just another opportunity, it can ultimately be determined what kind of policy changes are necessary to avoid inappropriate response by intergovernmental institutions.

Chapter two sets out the theoretical framework for this study. This can be considered the building blocks for conducting this research. It will clarify the used terminology, explain the relevant theories and concepts in order to build an analytical framework for consistency purposes. In chapter three, the methodology of this study is described and further explained. The next chapter presents the results of this study with a comprehensive analysis of the obtained data. Chapter five presents the conclusion and discussion, and chapter six includes the recommendations. Lastly, chapter seven elaborates on the limitations of this research.

2. Theoretical framework

To understand and explain how cybercriminals exploit opportunities during the COVID-19 crisis targeting the healthcare sector, a theoretical framework is established for this research. This theoretical framework defines, explains and evaluates relevant theories and concepts based on criminological theories, such as the crime opportunity theory, and the routine activity theory – a subfield of the crime opportunity theory. The main purpose is to explain the key concepts, models and assumptions that are considered to be relevant to this research.

First, ransomware as a term is briefly explained by placing it into a broader context of cybercrime. Since the definition of cybercrime varies among jurisdictions and it can be perceived as a collective name for a diverse number of offenses, an explanation is provided on what cybercrime is and which types of cybercrime exists. Eventually, it will lead to an explanation of what ransomware is. Secondly, this study elaborates on the crime opportunity theory, specifically the routine activity theory, situational factors and the crime script analysis to provide this study with a framework of analysis to investigate how cybercriminals exploit opportunities. Finally, this section ends with a research question.

2.1. Ransomware: a cyber-dependent crime

Even though cybercrime is a broadly used term, varied views of what it actually is exist (Gordon & Ford, 2006). Its definition depends upon the purpose of using the term (UNODC, 2013) or it differs due various factors such as the perceptions of different people, for example the victim's or observer's perception, or they might differ depending on the purpose of the crime, the motivation of the perpetrator or the target of the crime. What also complicates having a unified definition of cybercrime, is that the definition varies among jurisdictions. For instance, what is criminalized in The Netherlands, might not be criminalized in India. This also creates difficulties whilst developing a categorization of cybercrimes and for conducting research especially if one compares data among countries. Cybercrime's definition can be a wide spectrum such as anything that leaves a digital trace, or it can be very narrow. Nonetheless, the core of cybercrime comprises of "a limited number of acts against the confidentiality, integrity and availability of computer data or systems" (UNODC, 2013, p. 17). Taking into account the difficulties and the core of cybercrime, this research builds upon the following definition “any crime that is facilitated or committed using a computer, network, or hardware device” (Gordon & Ford, 2006, p. 14).

Definitions of cybercrime are often subject to a division. For instance, Gordon and Ford (2006) distinguished two types of cybercrime: Type I and type II. Type I cybercrimes are characterized with an entirely technical component where the perpetrator makes use of crimeware programs such as keystroke loggers, viruses or rootkits to gain access to a system. Type II cybercrimes are characterized with a less technical component whereby information technology facilitates a certain crime, such as cyberstalking or committing fraud.

A quite similar subdivision of cybercrime broadly used by researchers is cyber-enabled and cyber-dependent crimes. Cyber-dependent crimes can be seen as Type I cybercrimes; these types of offences can only be committed using a computer, computer network or other types of IT (McGuire & Dowling, 2013). Types of cyber-dependent crimes are hacking, DDoS and ransomware. By opposite, cyber-enabled crimes are ‘traditional’ offences that are facilitated by using computers, networks and other types of IT. These types of crimes can also be committed without the use of IT such as online harassment (Furnell, Emm, Papadaki, 2015). Thus, cyber-enabled crimes are Type II cybercrimes.

Koops (2014) approaches it a bit differently by subdividing cybercrime into three types of cybercrime, namely computer-focused, computer-related, and computer-relevant crime. These categories are based on how information technology is used to commit a crime. Computer-focused crimes are crimes whereby the information technology itself is the target, such as hacking or a DDoS attack. If a computer is the substantial tool used to commit the crime, according to Koops (2014) is falls under the computer-related crime category. Lastly, computer-relevant crimes are crimes in which computers are there to facilitate a crime, for example to safe child pornography on a laptop.

Even though all three previously mentioned subdivisions have their own pros and cons, the subdivision cyber-enabled and cyber-dependent crimes is used for simplicity and understandability purposes. As cyber-enabled and cyber-dependent crimes together equals a broad spectrum of cybercrimes, this research narrows down the scope by focusing only on cyber-dependent crimes. More specifically, this research focus is on ransomware due to its nature and the severe impact it can have on the healthcare sector during the COVID-19 pandemic. The dependence of the healthcare facilities on its IT systems and reliable patient data makes them a suitable target for ransomware attacks (Boddy et al., 2017). Especially now, during the pandemic, the panic in combination with the criticality of these facilities might create opportunities for cybercriminals.

During a ransomware attack, malicious software is installed on a computer or IT-system with the primary goal to extort ransom payment from the targets by either blocking access to files or encrypting these files which is also known as cryptoware (Demuro, 2017; Crowdstrike, 2019; Nithya, Vijaya, Subramanian, Balamurugan & Shanmugavel, 2020). According to Cambridge Dictionary ("ransomware", n.d.), ransomware is "software designed by criminals to prevent computer users from getting access to their own computer system or files unless they pay money". Some types of ransomware even lock the user out from the system, also known as locker ransomware. Ransomware typically disables specific programs or functions of a system or the entire system. The cybercriminals may target any computer users, such as a home computer, endpoints in an enterprise network or servers used at a healthcare organization or government agency (Nithya et al., 2020). Whilst disabling programs, functions or the entire system, a message will appear on the system demanding a ransom payment in exchange for regaining the access to the system or its functionalities (Demuro, 2017; Crowdstrike, 2019; Nithya et al., 2020), or to fulfil a certain task that benefits the cybercriminal (Nithya et al., 2020). Another quite similar variant is scareware. Scareware does not actually encrypt files, but its purpose is to make the target believe that files or directories are encrypted to force them in paying money (Crowdstrike, 2019; Cybereason, 2020).

2.2. Opportunity makes the thief

Since a long time, researchers recognize that crime is typically opportunistic (Cohen and Felson, 1979; Yar, 2005; Holt & Bossler, 2008; Holt, Van Wilsem, Van De Weijer, & Leukfeldt, 2020) and this also applies to cybercrime. For instance, hackers frequently look at crises as an opportunistic perspective and the COVID-19 pandemic is no difference (Jagatic, Johnson, Jakobsson & Menczer, 2007). The pandemic provides a perfect opportunity to get a glimpse into how context can influence cybercrime.

The well-known criminological theory "routine activity theory" can be seen as a method to understand the ecosystem of cybercrimes as it clarifies the occurrence of high trends in crime rates due to changes in the routine activities of life. The theory in a nutshell: it explains that a crime is most likely to take place when a motivated offender found a suitable target in the absence of a capable guardian (Cohen and Felson, 1979). Because the internet has structural limitations to capable guardianship that can serve as a hindrance to commit crime, according to the theory the likelihood of the occurrence of a cybercrime increases. Guardianship refers to the capability of a person or an object to prevent crime from occurring (Yar, 2005).

In cyberspace, crime can be prevented by software solutions like firewalls, intrusion detection systems and virus scanning software. In this context, these can be interpreted as capable guardians (Yar, 2005; Clough, 2015). In context of the pandemic, such capable guardians can be absence since working remotely require different security solutions, like a virtual private network (hereafter, VPN), compared to working in a secured local office environment. Also, hospitals are experiencing many problems with its information security as relying on traditional security models to safeguard their systems has proven to be ineffective (Boddy et al., 2017). For instance, the usage of cryptographic techniques to protect medical data is often too expensive in terms of processor usage and power consumption. Therefore, it often is an unrealistic approach for certain medical devices or systems (Boddy et al., 2017).

The second component of the theory, a motivated offender, in the context of the pandemic can refer to changes to someone's life. Becoming unemployed can be a motivator for committing cybercrime. Especially during these circumstances, where many have become or will become unemployed, this might bring them closer towards committing cybercrime.

Lastly, working remotely also corresponds to more suitable targets. Even so, some studies show that situational factors are causing people to become more vulnerable as they lower their guard and therefore become suitable targets for victimization (UNODC, 2013; Holt et al., 2020). In addition, the leak of security coupled with the importance of the healthcare sector during the pandemic makes them a very suitable target for a ransomware attack.

Situational factors also influence the process of target-selection. For instance, according to a study conducted by Naidoo (2020), cyber criminals seek to take advantage of people who use social media to connect with each other. This study was an analysis of 185 unique documents and records of COVID-19 related cybercrime between mid-March and mid-April. These documents and records were supplied by FraudWatch International, an organization who collects cybercrime data globally. The results of this study showed that 39 % of these cases used a fake social network service to commit cybercrime. Other situational factors are working remotely, being unemployed, stay-at-home orders, online shopping, donations, safety measures and airline booking refunds (Naidoo, 2020). Opportunistic offenders always seek to maximize their gain, and therefore, will wait for the best time to attack where conditions are optimal (Lallie, Shepherd, Nurse, Erola, Epiphaniou, Maple & Bellekens, 2020). Hence, an ongoing crisis such as the COVID-19 pandemic is the perfect example wherein particular situational factors coupled with panic influence target-selection.

Following the crime opportunity theory, the routine activity theory and situational factors, a ransomware attack towards the healthcare sector is certainly not a surprise given the crucial nature of this sector. Disabling a healthcare organization's IT systems, its functionalities or data can threaten patient care and therefore create maximum urgency to pay the ransom.

2.3. Modus operandi and crime script analysis

Finding out what motivates cybercriminals has kept researchers and law enforcement busy for quite some time. By classifying offenders and their motivations, it not only enables us to efficiently identify threats based on existing knowledge of offender types, but it also improves our understanding of such adversaries (Seebruck, 2015). With the acquired knowledge, organizations will be able to improve their incident response and crisis management strategy. According to Boin and McConnell (2007) crisis preparedness as a strategy for containing emergencies is crucial to maximize predictability. In addition, as it is not achievable to prepare for all types of cyber threats, organizations will have to decide on which threats to eliminate by means of a proper risk management strategy.

One of the most cost-efficient risk management strategies is to create attacker profiles stating the level of skills of these offenders (Buyens, De Win & Joosen, 2007). Such attacker profiles facilitate reporting of cyber incidents. This is crucial because detailed records of cyber incidents can lead to the discovery of new security threats, which in return can help organizations to stay ahead of cyber threats (Seebruck, 2015). Conversely, investigating cyber offenders' motives can be problematic due to the leak of sufficient digital evidence left behind to identify the cyber offenders or their country of origin (Nurse, 2018). As such, this study focuses on modus operandi excluding motivations.

According to the Cambridge Dictionary ("Modus operandi," n.d.), modus operandi is a particular way of doing something. In this context, it can be interpreted as a way of committing cybercrime, also referred to as the method. In principle it means that an offender is likely to use the same technique repeatedly and it is dependent on multiple variables such as knowledge and habits of offenders or victims, the availability of technology for both offenders and victims, and laws, rules, or regulations that govern the technology and behavior of people. Typically, the modus operandi consists of a few elements to classify the technique such as target, scene, the point of entry, tools, time of day, style or trademark of the offender (Newburn, Williamson & Wright, 2007).

The identification of the modus operandi helps to seek an answer to the 'how' question. As part of identifying the modus operandi, this research takes a closer look at the attack methods of cybercriminals deploying ransomware. In doing so, crime script analysis will be used as a tool in order to analyze the attack methods and thus the modus operandi. It helps to identify what types of criminal opportunities the COVID-19 pandemic offers for ransomware attacks and how these opportunities affect the way a ransomware attack is executed.

In this research, the modus operandi will be discovered by means of a crime script analysis. In essence, crime scripts are models to identify the sequence of steps which are carried out for a criminal activity to occur (Dehghanniri & Borrion, 2019) and it makes the crime-commission process significantly easier to identify and understand (Leclerc, 2017). As these crime scripts play an important role in identifying step-by-step exploited crime opportunities, in return it provides potential for analysis and prevention (Lavorgna, 2018a). While identifying opportunities, potential points of intervention can be conceived. More specifically, "situational crime prevention teaches us to think about a crime by breaking it up into the sequential phases of its commission" (Lavorgna, 2014, p. 3).

Crime script analysis is a successful approach for conducting criminological research (Lavorgna, 2014) as it is used to enhance the understanding of not only conventional crime but also cybercrime (Lavorgna, 2014; Hutchings & Holt, 2015; Dehghanniri & Borrion, 2016). Most importantly for this research, crime scripts analysis provides both a framework and a method for investigating how a ransomware attack is carried out targeting the healthcare sector during COVID-19 and to determine whether this changed compared to the situation before the pandemic. With this knowledge, points of intervention can be established to help the healthcare sector gain resilience for future ransomware attacks.

2.4. Research question

This qualitative research examines to what extent the COVID-19 pandemic offers new opportunities for offenders to commit a ransomware attack targeting the healthcare sector. More specifically, it first seeks to investigate how a ransomware attack is carried out at healthcare organizations during the pandemic through conducting a crime script analysis. As such, this study attempts to identify what steps are required for offenders to deploy a successful ransomware attack at the healthcare industry during the pandemic. Subsequently, it then investigates whether this differs from the situation before the COVID-19 pandemic. The research question is: “To what extent did the COVID-19 pandemic change the modus operandi of offenders deploying a ransomware attack at the healthcare sector?”

3. Methodology

The existing literature on this topic has laid a foundation for understanding the theoretical background of the research object and the crime script analysis, as well as the importance of the opportunity and routine activity theory in this context. The scope of this research comprises of ransomware attacks targeting the healthcare sector since the WHO declared COVID-19 a pandemic on 11 March 2020 (Ducharme, 2020).

Furthermore, the objective of this research is three folded: firstly, its aim is to determine to what extent the COVID-19 pandemic offers new opportunities for cybercriminals to commit a ransomware attack targeting the healthcare sector. Additionally, the secondary objective of this research is to discover techniques of ransomware deployment in order to help the healthcare sector in becoming resilient. The third objective is to investigate whether the claims regarding the changing nature of ransomware are justified or whether this is a case of moral panic.

3.1. Design of the study

In order to meet the abovementioned objectives, the focus of this study is on qualitative research. More specifically, it first examines in detail how offenders exploit opportunities by deploying ransomware targeting the healthcare sector during the COVID-19 pandemic, starting from 11 March 2020 when the WHO declared COVID-19 a pandemic (Ducharme, 2020). Afterwards, it examines to what extent this differs from the situation before the COVID-19 pandemic. Qualitative studies' strength lies in the analysis of situations within their context; thus, it takes into account the situational factors influencing the process of target-selection for ransomware as it "investigates a contemporary phenomenon within its real-life context" (Yin, 2003, p. 13).

In order to aim for a structured and consistent approach for data collection and analysis, crime script analysis was used by relying upon the crime scripting process model of Dehghanniri and Borrion (2016). This model, as represented in Figure 1, provides guidelines to support the analysis in the use of a more systematic crime scripting method. The model should not be seen as linear as it is not necessarily to follow or include all eight stages in generating a crime script. These stages can be repeated or omitted if deemed to be necessary.

During the first stage the crime phenomenon subject to the analysis is identified including the purpose of analyzing a crime script. The purpose of the second stage is to determine the requirements for collecting information taking into consideration the application of the crime scripts. These requirements can be divided into two categories: "(1) those specifying what types of states, events, or activities should be modelled and (2) those specifying what aspects of those states, events, or activities should be detailed" (Dehghanniri & Borrion, 2016, p. 95). During the Data Source Selection stage, the relevant data sources for collecting the information will be determined taking into account the previously mentioned information requirements. Furthermore, the purpose of stage 4 is to assess and improve the quality of the collected data in order to identify whether additional data is required for reliability or completeness purposes. Stage 5 aims to identify and extract relevant information from collected data sources by focusing on the information requirements as identified at stage 2. During the next stage a visualization model is chosen, such as narratives, flowcharts or tables, to represent the crime script. Next, in stage 7 the information will be organized to construct the crime script alongside with reviewing and re-wording to improve the script. The purpose of the last stage is to evaluate the generated crime script to assess whether the selected list of criteria is met (Dehghanniri & Borrion, 2016).

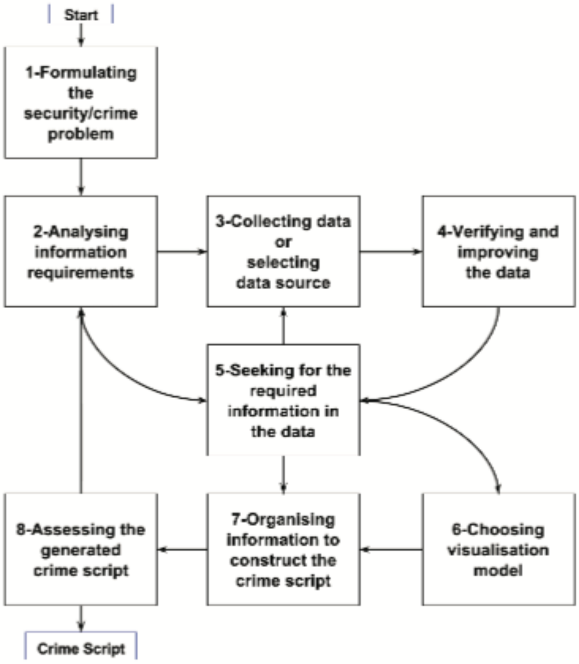

Start
1-Formulating the security/crime problem
2-Analysing information requirements
3-Collecting data or selecting data source
4-Verifying and improving the data
5-Seeking for the required information in the data
6-Choosing visualisation model
7-Organising information to construct the crime script
8-Assessing the generated crime script
Crime Script

Figure 1. Adapted from "Toward a more structured crime scripting method," by Dehghanniri, H., & Borrion, H., 2016, 2016 IEEE 24th International Requirements Engineering Conference Workshops, p. 94-98.

Based on the above-mentioned crime scripting method, a security problem was formulated and discussed in the previous chapters. After that, the following requirements are established to search for appropriate data:

1) Both successful and unsuccessful ransomware attacks are included because unsuccessful attacks also contain valuable information
2) The ransomware attack must have targeted the healthcare sector
3) The ransomware attack must have taken place after 11 March.

Furthermore, the third stage of the model was not fully incorporate. Data source were not always determined beforehand but were often selected through searching in the University's Library, Google Scholar or based on references in papers. The approach for collecting data is further discussed in chapter 3.2. After the identification of the crime-commission process through the crime script analysis, literature and other data source are used to analyze whether new opportunities have arisen. This analysis was complemented by Interviews for validity purposes.

3.1.1. Framework for analysis: the crime script

Through the crime script framework and the literature review, it was possible to create a crime script by reconstructing the important steps taken by offenders to deploy a ransomware attack at the healthcare sector during the COVID-19 pandemic. A total of 43 data sources were used to identify the crime-commission process, including reports from Kaspersky, the Dutch Police, Europol, Interpol, FBI, Palo Alto, TrendMicro, Intsights, McAfee, Varonis, Advanced Intel, CoveWave, Cybereason, Bitdefender, Crownstrike, Phishlabs, Avast, ICANN, Cyware, and Microsoft. This has resulted in a crime script consisting of six stages. The result chapter is structured by using the identified stages of a ransomware attack, namely 1) preparation, 2) initial access and compromise, 3) command-and-control, 4) exploring and expanding, 5) encrypting files, directories or systems, and 6) extortion and monetization. The crime script is presented in the below picture.

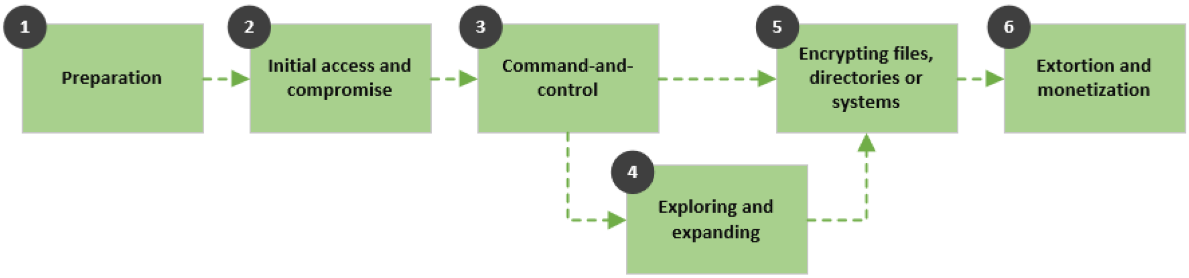

1
Preparation
2
Initial access and compromise
3
Command-and-control
4
Exploring and expanding
5
Encrypting files, directories or systems
6
Extortion and monetization

Figure 2. Crime script of ransomware attack targeting the healthcare sector during the corona-era

During the first stage, the attacker is preparing the attack by taking into consideration which ransomware family, methods and tools used to conduct the attack. After that, the attacker will need to find its way into the system by compromising the system. This can be accomplished through phishing emails, a brute force attack or through the exploitation of internet-exposed services and public-facing applications. The third stage describes how the attacker controls the malware or ransomware through the establishment of a command-and-control (hereafter, C2) communication channel. The next stage, the exploring and expanding stage, is not always part of a ransomware attack as also shown in Figure 2. During this stage, the attacker explores the network to determine the most valuable data to increase the impact of the attack. In this case, the attacker uses a more sophisticated and stealthy method to avoid detection. Then, in the fifth stage, the attacker runs the ransomware and encrypts the files, directories or systems as determined by the attacker. After successfully encrypting the files, directories or systems, in the last stage the attacker will both choose a way of extorting the victim and determine a payment method to receive the ransom from its victim.

3.2. Data collection

Examining attack methods and modus operandi is not easy whilst using conventional research approaches (Naidoo, 2020). As such, researchers will have to build their research on secondary data to get a glimpse of cybercrime as a phenomenon. Consequently, this empirical research includes widely spread types of text-based, secondary data sources to foster a helicopter view. These sources can be categorized into open-source data and interview data.

Open-source data consists both of relevant academic sources and non-academic sources that are publicly available, such as law enforcement statements, scientific papers, evaluation reports from the public and the private sector, and journalistic items. These are collected through Leiden University's database, Google Scholar, the website of the following:

Kaspersky, the Dutch Police, Europol, Interpol, FBI, Palo Alto, TrendMicro, Intsights, McAfee, Varonis, Advanced Intel, CoveWave, Cybereason, Bitdefender, Crownstrike, Phishlabs, Avast, ICANN, Cyware, and Microsoft. Whilst collecting the data, the requirements as established through the crime scripting method were providing guidance and structure. The search was conducted through two mechanisms: firstly, through keyword search (using the term 'COVID-19' or 'corona' in combination with 'ransomware' and 'hospitals' or 'healthcare') of relevant data sources including grey literature and dissertation databases. Secondly, through forward citation search based on the primary article in this area (Cornish, 1994b). In some cases, if the source did not provide any detailed information on the ransomware attack, additional sources were used to investigate the particular ransomware family.

The other data sources consist of the transcripts of the three interviews conducted with experts such as an analyst from a commercial threat intelligence provider, an IT security manager from a Dutch hospital, and a researcher from the Dutch police. Interviews were included to validate the findings of the analysis of open-source data and to obtain additional information. In Table 1, an overview of the respondents is provided, together with their occupation. To respect the respondents' privacy, they are anonymized throughout this research.

Reference	Occupation
Respondent 1	Forensic analyst at an international commercial threat intelligence provider
Respondent 2	IT security manager at a Dutch hospital
Respondent 3	Researcher at the Dutch police

Table 1: Overview of the respondents

Interviews were included to validate the findings of the analysis of open-source data and to obtain additional information. The participants were selected through non-probability sample methods, namely purposive and snowball sampling. The former method allowed a search for participants who are knowledgeable about ransomware at the healthcare sector, willing to talk and with varied expertise, and the latter allowed reliance on the initial element contacts to provide additional participants. In doing so, a semi-structured approach has been the starting point for the interviews. This was the preferred approach because it provides comparable qualitative data and it encourages the participants to express their views in their own terms (Yin, 2003; Yin, 2012).

> 'The flexible format permits open-ended interviews, if properly done, to reveal how case study participants construct reality and think about situations, not just to provide the answers to a researcher's specific questions and own implicit construction of reality' (Yin 2012, p. 12).

A number of interview questions were established upfront to use as a guideline for consistently conducting the interviews. These questions are presented in appendix 1. Depending on the background and the experience of the participant, some questions were not discussed, or additional questions were asked.

Lastly, due to the fact that the COVID-19 pandemic is an international matter, the aim of this research is to incorporate literature from various countries. However, only literature written in English or Dutch are included.

3.3. Data analysis

A multitude of sources is used through a combination of literature review and the analysis of the interview data to provide an answer to the main research question. By doing so, the reliability of the findings is increased (Talja, 1999). The main purpose of the interviews was to strengthen the results of analyzing the open-source data and to obtain additional information on what is observed in practice.

Furthermore, an analytical framework has been constructed, through the crime script analysis, in order to analyze the data obtained through literature review and present the important steps taken by offenders who committed a ransomware attack at the healthcare sector. The interviews were included to strengthen the analysis of data collected from literature, documents and reports. Additionally, the analytical framework consists of the stages and elements that are relevant for understanding how offenders deploy ransomware at the healthcare sector during the COVID-19 pandemic. Ultimately, through additional literature review and interviews, it was investigated if the pandemic has an impact on ransomware attacks.

The documents were thoroughly read and interpreted. Both content and thematic analysis were used as a method for analyzing the data sources. According to Bowen (2009, p.32), content analysis is the "process of organizing information into categories related to the central questions of the research". As such, the documents were reviewed at a high-level to distinguish relevant from non-relevant texts and text-passages. Thematic analysis is "a form of pattern recognition within the data, with emerging themes becoming the categories for analysis" (Bowen, 2009, p. 32). This method was used for prudently re-reading of the selected information as identified through content analysis. By this means, the purpose was to construct the crime scripts and to identify the corresponding stages and elements.

3.4. Limitations of research methodology

Although qualitative research has its advantages, such as gaining a thorough understanding of a certain phenomenon, it also has some drawbacks. Lack of generalizability is the main limitation of qualitative research as the results cannot be extended to wider populations. Unlike with quantitative research, the results of the qualitative research are not tested to determine whether they are statistically significant or due to chance (Queirós, Faria & Almeida, 2017).

Another difficulty whilst conducting this research is obtaining sufficient and reliable data. Data sources might not contain information that could be relevant for the context of this research or it might provide the wrong impression. Also, data sources such as reports regarding cyber security from professional service firms or security software solutions might also be questionably due to the commercial interests of those firms.

Furthermore, another limitation of qualitative research is that it can be difficult and complex to analyze and interpret the results. Whereas quantitative research is characterized with objectivity, qualitative research is mainly characterized with subjectivity (Queirós, Faria & Almeida, 2017).

Even though interviews are a valuable source of data, it is also sensible for researcher bias. According to Galletta and Cross (2013, pp. 103), "the interaction between the researcher and participant has the potential to yield disjunctures in meaning and intent". In order to minimize or avoid researcher bias, the interviews were held after the literature review has been conducted and processed in this research. This contributes to the level of knowledge, making it easier to conduct and interpret the interviews. The results of the literature review were used as a guideline for conducting the interviews.

Lastly, crime scripts are often reconstructed based on secondary data sources that do not necessarily contain all the relevant aspects of the crime script, and their reliability could be limited. As such, the more information, the more reliable the crime script (Dehghanniri & Borrion, 2016).

4. Results

As briefly explained in the previous chapter, this particular section is structured through the established crime script of a ransomware attack during the pandemic targeting the healthcare sector, namely: the preparation stage, the initial access and compromise stage, the command-and-control stage, the exploring and expanding stage, the encrypting files, directories or systems stage, and lastly the extortion and monetization stage.

4.1. The preparation stage

The first stage as identified through the literature review was the preparation stage. This stage represents the steps taken by attacker to prepare for deploying the ransomware on the target's IT systems. During the preparation stage, offenders will typically identify suitable targets, ransomware family, the methods and tools used to conduct the attack (Crowdstrike, 2019). Because of the limited information on how offenders identify suitable targets in the context of the healthcare sector, the preparation stage will only address the usages of tools.

The identification of suitable tools refers first of all to the decision on whether own means and abilities will be used for the attack or whether to buy the means from other criminals for instance through the Dark web. Also, the attacker might decide to outsource the required activities by paying another criminal to conduct it as a service (Somer, Hallaq & Watson, 2016).

Secondly, the attacker will have to determine which ransomware family, methods and tools will be used for conducting the attack. The tool can refer to registering a domain name, developing or purchasing the malware used to control the infected system, and acquiring the ransomware used to extort the target. Also, the attacker will need to consider the method for deploying the malware and ransomware on the target's system such as through the use of phishing mails or through exploiting a vulnerability. These methods are discussed in more detail in the execution stage.

4.1.1. Domain name registration

An important element of a ransomware attack is to establish a C2 communication channel to both send data to and receive instructions back from the attacker (Vissers et al., 2017; Interpol, 2020). C2 communication often happens over the internet and to make this happen, the attacker will need to register a domain name also referred to as a malicious domain name. These malicious domain names are often used for establishing C2 communication, malware distribution and phishing (Vissers et al., 2017; Szurdi, Chen, Starov, McCabe & Duan, 2020). Such a C2 domain is, for example, used by malware for receiving commands and for data exfiltration (Szurdi et al., 2020).

Interestingly, quite some reports, articles or statements (Check Point, n.d.; Interpol, 2020; Mahadevan, 2020; Szurdi et al., 2020) claim that during the pandemic explosively more domains were registered or that newly registered domains containing a COVID-19 related term were identified more often as being associated with criminal activities such as malware distribution, scams and phishing. Also, according to Check Point (n.d.), a security software provider, COVID-19-related domains are 50% more likely to be malicious than others registered throughout the same period. In contract to these claims, the Council of European National Top-Level Domain Registries (hereafter, CENTR) (2020) has investigated the effect of the COVID-19 crisis on the DNS. This was done through analyzing domains which included COVID-19 related terms for the period of January to March 2020. In total of 6,164 registrations were identified as COVID-19 relevant. Then, CENTR (2020) identified a total of 751,000 new domains that were registered in the same three-month period. They concluded that domains with a COVID-19 related term represent only 0.8 percent of all newly registrated domains in this period, thus their results show that the pandemic has had no significant impact on the DNS registrations. Additionally, CENTR (2020) also investigated how the newly COVID-19 domain were used and concluded that the pandemic also has had no significant impact in levels of abuse detected than what they normally observe (CENTR, 2020).

Because domain names are required for all communication on the web along with the fact that in the past, attacker have launched cyberattacks close to or during momentous world events which were made possible through registered malicious domains (Jackson, 2005; Greenberg, 2008; Guerra, 2009; Thornton, 2009; Tuluc, 2011; Verma, Crane & Gnawali, 2018), it cannot be seen as a new opportunity used by offenders to deploy a ransomware attack (Gostev, Zaitsev, Golovanov & Kamluk, 2008; Vissers et al., 2017). Moreover, reports on the effect of COVID-19 on domain names are quite contradictory and mostly incomplete. The Internet Corporation for Assigned Names and Number (hereafter, ICANN) for instance report that around 8 percent of the registered COVID-19 domains were identified as malicious (Lloyd, 2020). However, they did not put this into a broader perspective by comparing the results with the situation before the pandemic which makes it difficult to determine whether this is an abnormal situation. As such, more quantitative research is required to determine whether there truly is a significant relationship between COVID-19 and newly registered malicious domain names to assess whether this actually poses a problem.

4.1.2. Tools

In order to compromise the target's system or deploying ransomware, various tools are used. Offenders sometimes make use of legitimate commercial off-the-shelf products such as PowerShell Empire or Cobalt Strike, which were established in 2012 (CobaltStrike, 2012), to steal valid credentials or to establish a communication channel. In a conversation with respondent 1, he emphasized that Cobalt Strike is quite a popular legitimate tool used amongst criminals.

Other tools used to compromise a system and deploy ransomware are TrickBot trojan[1], BazarLoader, AgentTesla, BloodHound and LaZagne. The TrickBot trojan is frequently used as the primary hacking tools for conducting the cyberattacks on the healthcare sector during the pandemic (Newman, 2020; CISA, 2020). Beforehand, the TrickBot trojan was a banking trojan but it now offers a set of tools to conduct a variety of illegal cyber activities such as crypto mining, credential harvesting, mail exfiltration and the deployment of ransomware (CISA, 2020). The TrickBot trojan is often used in combination with Ryuk ransomware (CISA, 2020). Another tool used during the COVID-19 pandemic for conducting a ransomware attack on the healthcare sector is BazarLoader, or also known as BazarBackdoor. According to Marhanksi and Kremez (2020), offenders targeting the healthcare sector during the pandemic now favor BazarLoader over TrickBot trojan because it is more difficult to detect than TrickBot. Respondent 1 added: "if you see Ryuk, nine times out of ten BazarLoader is deployed just before the ransomware". With this statement, it becomes clear that BazarLoader is an important tool for the Ryuk ransomware family.

Most of these identified tools were already on the market before the pandemic; the only exception is BazarLoader which was first spotted in April 2020 (Cyware, 2020; Hall, 2020; Marhanksi & Kremez, 2020). Respondent 1, the forensic analyst, also emphasized that BazarLoader is fairly new. In contract to BazarLoader, AgentTesla is a malware that has been infecting IT systems since 2014 (KrebsonSecurity, 2018; Gittins & Soltys, 2020). The malware enables offenders to steal passwords saved in browsers, collect keystrokes and take print

[1] A trojan is a type of malware that conceals its true purpose from computer users, who are fooled into downloading it believing it is legitimate software (Mahadevan, 2020, p. 7).

screens of the victim's computer (Gittins & Soltys, 2020). Furthermore, similar to Cobalt Strike and LaZagne, BloodHound is a tool developed by or for penetration testers. This tool is used to is to obtain a comprehensive picture of a network environment and to identify the relationships that would eventually facilitate obtaining privileged access, such as to get Active Directory domain admin access (Bertram, 2019; Mallon, 2020). The tool was first released in 2016 (Wald0, 2016; GitHub, n.d. a). Moreover, LaZagne is an open-source application which is used to retrieve passwords stored on a local computer and it has been developed for the purpose of finding passwords for the most commonly used software. The first version was release in 2015 (Son, 2019; GitHub, n.d. b). Lastly, PowerShell Empire's initial release date was in 2015 and it is a post-exploitation framework (GitHub, n.d. c).

Thus, offenders mostly used already existing tools in their attacks on the healthcare sector. The only exception was BazarLoader. Whether or not it is a coincidence that BazarLoader showed up during the pandemic is not clear. There has not been any evidence that BazarLoader was developed specifically for pandemic-related ransomware attacks. It requires additional research to determine whether there is a significant relationship between the release of BazarLoader and the COVID-19 pandemic.

4.1.3. Ransomware families

Ransomware can be classified into groups by using different criteria. Often, they are classified into families according to its code signature, which contains the sequence of instructions and commands of those who are responsible for the malicious action (Subedi, Budhathoki & Dasgupta, 2018).

According to some reports (Advanced Intel, 2020; Frank, Zhao & Dahan, 2020; Newman, 2020; McAfee, 2020; Interpol, 2020), the top ransomware families detected in the corona-era are Maze, Ryuk, Cerber and NetWalker. These are constantly evolving to maximize the potential damage as well as the profit for the offenders. Interestingly, is that these ransomware families were already on the market before 11 March 2020 when the WHO declared COVID-19 a pandemic (Advanced Intel, 2020; Ducharme, 2020; Palo Alto, 2020). For instance, the Ryuk ransomware first appeared in August 2018 as a derivative of another ransomware namely Hermes 2.1, which first emerged in 2017 and was available for sale as of August 2018 (Hanel, 2019; CISA, 2020). In September this year, the Ryuk ransomware was used as a tool to target the Universal Health Services which is a hospital and healthcare network with more than 400 facilities across the United States, United Kingdom and Puerto Rico (Newman, 2020).

According to Intel471 (2020), Ryuk is one of the biggest threats this year for the healthcare sector. This was also confirmed by all the participants during the interviews. Participant 1 labelled the Ryuk-gang hunt as “a sort of big-game hunting” but he did also mention that it is a little bit on the down-climb instead of uptilting. The gang is known for its high ransom demands which makes forensic analysts and researchers to focus their investigation on them. Another ransomware family, namely the open-source ransomware variant EDA2, is associated with a ransomware family called HiddenTear (Palo Alto, 2020) and was already on the market before the pandemic (Europol, 2016; TrendMicro, 2016). The ransomware payload is delivered through using a known shared Microsoft component vulnerability (Palo Alto, 2020). Moreover, the NetWalker ransomware was first spotted in August 2019 but now has become remarkably active through targeting hospitals (Advanced Intel, 2020).

The above-mentioned indicates that cybercriminals continue to develop new functionalities and improve already existing ransomware at any time to increase the speed, ease and profitability. Most of the identified ransomware families were already active before the pandemic: Maze ransomware has been active since May 2019 (Sophos, 2020), Ryuk since August 2018 (Hanel, 2019; CISA, 2020), NetWalker since August 2019 (Advanced Intel, 2020), EDA2 since 2016 (Europol, 2016; TrendMicro, 2016), and Cerber was developed somewhere between 2015 and 2016 (KnowBe4, n.d.; Zahra & Shah, 2017; Meskauskas, 2020). Additionally, respondent 1 explained that he did not really see Maze as much as he saw SunCrypt, which is a variation of Maze. The malware family itself is very much similar from a source code perspective, but the operators behind it differ. He further indicated that they have seen SunCrypt aiming at the healthcare sector this year. The SunCrypt gang began operating in October 2019 (Abrams, 2020). Another type of ransomware that has burdened hospitals during the pandemic is REvil, also known as Sodinokibi (Paganini, 2020; Stafford, 2020) and was first spotted in April 2019 (Secureworks, 2019).

As previously mentioned, most of the ransomware families were already on this market. However, whilst Maze recently shutdown their operations, a new family, Egregor, has emerged claiming that they have targeted a hospital (Davis, 2020). This was also confirmed by respondent 1 during the interview. He added: “we have seen a huge influx of their ransomware being deployed across all sectors within the last months. It is sort of the popular flavor for cybercriminals right now".

Netwalker, REvil, Egregor and Cerber are typically provided as so-called Ransomware-as-a-Service (hereafter, RaaS) (Advanced Intel, 2020; Belcic, 2020; McAfee, 2020; Petters, 2020; Victor, 2020). This means that the ransomware developers either lease or sell the ransomware variants to the offenders who will use the ransomware to perform the attack. The offenders often will need to split the ransom with the RaaS provider (Advanced Intel, 2020; Belcic, 2020; Conti, Gangwal & Ruj, 2018; McAfee, 2020; Petters, 2020; Victor, 2020). This allows individuals without the required knowledge or skills to become active offenders (Conti, Gangwal & Ruj, 2018). However, RaaS is not a new way of ransomware deployment as this already existed before the pandemic (Richardson & North, 2017; Conti, Gangwal & Ruj, 2018; Intel471, 2020). As stated earlier, the RaaS ransomware Cerber was established around 2016 (KnowBe4, n.d.; Meskauskas, 2020), Netwalker in August 2019 (Advanced Intel, 2020) and REvil got on the market in April 2019 (Secureworks, 2019).

In a conversation with respondent 1, it was mentioned that cybercriminals do see the value of RaaS resulting in an up climb. However, whether this was caused by the COVID-19 pandemic, is difficult to say according to him. He did also indicate that working from home might have played a factor due to an increase in using vulnerable VPNs or having Remote Desktop Protocol (hereafter, RDP) exposed. Somewhat the same argument was made by respondent 3, she mentioned that there are many RaaS providers and that these are increasing but this was already on the rise since 2019 as criminals already saw the benefits of ransomware. Hence, RaaS was already on the rise well before the pandemic.

Ransomware families continue to evolve through the deployment of new features or even through the emergence of new families as technology is evolving quickly and offenders always look for a way to evade detection. Even though most of the ransomware families already existed before the pandemic, a new family Egregor did emerge in September this year (Davis, 2020; respondent 1, personal communication, December 9, 2020). Because there was already an upwards trend in RaaS schemes, there is yet no particular indication that the pandemic has led to the development of a new RaaS-schemed family.

4.2. The initial access and compromise stage

An important step in the modus operandi is how ransomware is deployed on an IT system in the first place. The attacker will need to gain access to the system before he can deploy a ransomware attack. Through analyzing the available data, there were three ways of gaining initial access and deploying ransomware identified: through phishing emails, a brute force attack or the exploitation of internet-exposed services and public-facing applications.

4.2.1. Phishing attack

One of the most common ways to gain control over an IT system is through phishing mails. Phishing is a form of social engineering as the perpetrator tries to convince the victim to share sensitive information by telephone or via an email (Davinson & Sillence, 2010; Bullée, Montoya, Pieters, Junger & Hartel, 2015). Phishing methods are becoming progressively sophisticated (Abraham & Chengalur-Smith, 2010; Davinson & Sillence, 2010). The email often appears to come from an organization containing name and address information obtained via the internet. Usually, the names and logos of medium to large sides organization are misused to make the email appear as real as possible. As such, potential victims often gain both confidence and trust that the content and sender of the email is valid (Abraham & Chengalur-Smith, 2010; NCSC, 2016).

According to some reports (CISA, 2020; Cybereason, 2020; Interpol, 2020; Marshanski & Kremez, 2020; Palo Alto, 2020), emails sent during the COVID-19 pandemic contained COVID-19 related information as a lure to gain the target's attention. Not only does phishing remains a popular method of obtaining information from individuals and organizations (Mitnick & Simon, 2002; Abraham & Chengalur-Smith, 2010; NCSC, 2016), but it is also used to spread malware to gain access to IT systems (Bossler & Holt, 2010; NSCS, 2016). For instance, during the pandemic offenders deployed TrickBot and BazarLoader via phishing emails. These emails either contained attachments with malware or links to malicious websites that actually host the malware and often contained COVID-19 related subjects (CISA, 2020).

Palo Alto (2020) also identified malicious emails using subjects containing COVID-19 or any related keywords to distribute malware or ransomware. These emails contained Remote Administration Tools (hereafter, RATs), also known as Remote Access Trojans, like LokiBot, NetWire, and NanoCore. An example of such an attack was noted by Palo Alto (2020) between 24 and 26 March 2020 whereby they observed several malicious emails sent from a spoofed address to several individuals associated with a Canadian health organization who are actively engaged in COVID-19 response efforts. The emails all contained a malicious file in Rich Text Format (RTF) with the file name 20200323-sitrep-63-covid-19.doc. If such a file is opened with a vulnerable application, the EDA2 ransomware can find its way through the user's system (McCabe, Ray & Cortes, 2020).

Various reports (Interpol, 2020; Mahadevan, 2020; McCabe, Ray & Cortes, 2020) reveal that a phishing attack was the most common used method of gaining initial access to a system during the pandemic. Before the pandemic, gaining access to a system was also mostly accomplished through phishing mails as this was the preferred method used by offenders (Chiew, Yong & Tan, 2018; Verma, Crane & Gnawali, 2018). A plea may be that there is certainly a difference compared to the situation before the pandemic; the topics of the phishing mails as they included COVID-19 related keywords. By this means, offenders misused the pandemic to increase urgency by including words related to COVID-19. However, knowing that crime is typically opportunistic, COVID-19 related keywords may as well be replaced by other keywords related to another disaster. The use of COVID-19 related keywords has not made a major change in the modus operandi, but it only provides additional options to lure the victims.

This is also refuted by a research conducted by Verma, Crane and Gnawali (2018) revealed that offenders exploited the hurricane Harvey disaster to trick victims to either download or click on a URL in a phishing mail. In this case, offenders also misused the situation to include keywords related to the storm. Thus, the COVID-19 crisis is no difference to previous crises or events in terms of how cybercriminals use the opportunities.

4.2.2. Brute force attack

Another way to gain initial access to the target's system is through a brute-force attack. With a brute force attack, the attacker can obtain valid credentials to the target's system and log in. A quite commonly used method of obtaining valid credentials is through password-spraying brute-force attacks against internet-facing services such as Server Message Block (hereafter, SMB) and RDP. Password-spraying is a method whereby offenders try a small number of commonly used passwords to get access to an account. As organizations often fail to properly secure RDP accounts or services, for example by allowing accounts with RDP privileges to have a weak password, this could open the door for offenders to conduct a brute-force attack (Whitney, 2020). If successfully, the attacker could obtain valid credentials to invade a network.

Once the attacker has access, a suspicious PowerShell command can be executed which will be used to request data from a remote host (Crowdstrike, 2020). This particular technique is used to facilitate network communications to C2 servers and is explained in the next stage.

Even though the method to execute a brute-force attack towards RDP is not new (Vizváry & Vykopal, 2013; Ivanov, 2014), the increase of individuals working remotely during the pandemic could contribute to the increase of ransomware attacks due to brute-force attacks against RDP (Whitney, 2020). This also creates more opportunities for offenders to deploy ransomware.

ESET, an organization providing security solutions, has observed a rise this year in reported RDP attacks from among their customers: from approximately 30.000 reported attacks per day in December 2019, to 100.000 in April 2020 (Kubovič, 2020). Others (Kaspersky, 2020; Pankov, 2020) also have observed an increase in RDP-related attacks. In addition, Faval, Soro, Trevisan, Drago and Melliaa (2020) conducted a research on whether the pandemic had an impact on the campus traffic to identify changes in malicious network activities. This was done through analyzing the network events visible from the campus' network security monitoring solutions. Their research concluded that the number of RDP events had more than doubled in the week of March 16th compared to the beginning of February 2020. Subsequently, some of the participants noted an increase in RDP-related attacks during the pandemic as well. These results can potentially indicate that the pandemic had a significant effect on the number of RDP-related attacks, such as brute-force attacks. However, it will have to be further investigated whether this is actually the case by increasing the scope and looking at changes compared to one or two years ago.

4.2.3. Exploitation of internet-exposed services and public-facing applications

Lastly, offenders also have the ability to exploit weaknesses in certain, particularly unpatched, internet-exposed services and public-facing applications. In some cases, this happened through misconfigured web servers, including electronic health record software, systems management servers or backup servers, or through vulnerabilities found in Citrix Application Delivery Controller systems or Pulse Secure VPN systems (Microsoft, 2020).

Additionally, weaknesses in RDP or Virtual Desktop endpoints without multi-factor authentication or usage of older platforms were also exploited by offenders to gain initial access (Crowdstrike, 2020; Microsoft, 2020). Often offenders use RDP port scans to find RDP applications deployed on the system. Knowing which RDP applications are being used makes it easier for the attacker to search for RDP vulnerabilities to exploit. For instance, in 2012 Microsoft published information on the discovery of vulnerabilities in Remote Desktop and when these vulnerabilities are exploited it allows remote code execution (Microsoft, 2012). During the conversation with participant 2, an IT security manager of a Dutch hospital, it became clear that hospitals are not known for having proper security measures implemented. He explained that patching the systems requires more time than desired. This makes the hospitals more vulnerable for attacks.

The above-mentioned is also reflected in the scientific research conducted by Kruse, Frederick, Jacobson and Monticone (2017). They analyzed 31 articles published between 2006 and 2016 to identify cyber threats and its relationship to the healthcare sector. The results reveal that the healthcare sector lags behind in cyber security. One of the areas healthcare organizations are struggling with, is continuously and consistently updating the software. This, together with the statement of participant 2, show that the healthcare sector was already vulnerable to attacks due to the poor security. The pandemic might have exacerbated this concern and demonstrated again how vulnerable the healthcare sector is, but this did not change the modus operandi.

Exploiting vulnerabilities of internet-exposed service and public-facing applications is also something we have seen before. In 2017 around 40 hospitals that are part of the UK's National Health Service were hit simultaneously by the WannaCry ransomware through a vulnerability in the SMB in Microsoft Windows that has been exploited by the offenders (Harkins & Freed, 2018). Most of the infected hospitals' devices were found to have been running the unpatched Microsoft Windows 7 operating system, hence the offenders could compromise the systems (Acronis, n.d.). However, as already described in the previous section, RDP-related attacks which also includes the exploitation of RDP or SMB related vulnerabilities, are on the rise. In summary, with an increase in people teleworking, the attack surface on RDP increased as well.

4.3. The command-and-control stage

After the system has been compromised through the methods mentioned above, it is necessary for the attacker to set-up a communication channel in order to effectively determine and execute the next steps. These might be exfiltrating data through the use of HTTP, HTTPS, or FTP (Quintero-Bonilla & Martín el Rey, 2020; Liska, & Gallo, 2017). For example, the EDA2 ransomware creates an HTTP POST request containing data such as the victim's username and host name (McCabe, Ray & Cortes, 2020). Additionally, tools such as remote connection tools like Virtual Network Computing or RDP can be used to establish a communication channel (Quintero-Bonilla & Martín el Rey, 2020; Liska, & Gallo, 2017).

The C2 server plays an important role as backbone in ransomware communication. If the victim's system is able to connect to the C2 channel, it will then execute any command issued (Zahra & Shah, 2017). Another way to establish a communication channel and to establish foothold is through the deployment of a Cobalt Strike beacon into the target's system memory. A beacon is commonly used to deploy ransomware on a healthcare organization's system (Goody et al., 2020) and it has multiple functionalities. A beacon is not only useful for this stage, but also for the next stage to move laterally through the network. Chapter 4.4 will further elaborate on the usefulness of a beacon in the exploring and expanding stage. The type of channels used to establish the C2 connection vary among ransomware-families or malware used as a tool to gain access to a system (Liska, & Gallo, 2017). Worth mentioning is that the malicious code on the victim's system is a client and the attacker's C2 server is referred to as the server (Liska, & Gallo, 2017).

Once the C2 communication channel has been set up, the malicious code needs to get instructions as it will reach out to its command server. Besides specifying which files should be encrypted or the time for starting the process, these instructions can also report back information to the attacker such as domain names, IP addresses or which anti-virus products are installed on the systems (Liska, & Gallo, 2017). Additionally, the C2 is commonly used to distribute the encryption keys to encrypt the victim's data (Gujraniya, Waseem, Ar & Singh, 2017). Ransomware can also be deployed without using C2, in that case the ransomware uses encryption keys that are hardcoded or generated locally, these keys are often used for all the infected hosts. This results in easily reverse engineering the malware binaries and finding the keys. By using C2, the ransomware receives the encryption keys from the C2 server hosted by the attacker thus making it nearly impossible to recover the keys (Gujraniya, Waseem, Ar & Singh, 2017). Chapter 4.5 will elaborate on what the encryption process looks like as this is part of a separate stage of the crime script.

The command-and-control stage is an indispensable step in the crime-commission process of a ransomware attack (Liska & Gallo, 2017). Without a C2 server it is possible to reverse engineer the malware binaries and find the encryption keys. As such, having a C2 server increases the impact of the ransomware attack. In early ransomware variants, the C2 server addresses were hardcoded in the binaries, which made it easy to find and block these addresses. Subsequently, the C2 servers could not spread the infection and encrypt files (Gujraniya, Waseem, Ar & Singh, 2017). Unfortunately, offenders were getting smarter by generating dynamic domain names and redirect their C2 servers to these dynamic addresses to evade security defense tools such as firewalls (Gujraniya, Waseem, Ar & Singh, 2017). C2 has been used by offenders for quite some time (Gujraniya, Waseem, Ar & Singh, 2017) and there is no indication that the pandemic has provided any changes in this step of the modus operandi. Thus, this stage may not be interpreted as a new opportunity but rather a crucial component to deploy a successful ransomware attack. This applies to any ransomware attack, not only during the pandemic at the healthcare sector.

4.4. Exploring and expanding

In most of the cases, the ransomware attack was more advanced and sophisticated. Instead of deploying the ransomware on the initial targeted system (e.g., with EDA2 and Cerber), offenders firstly explore the network by extracting information from the target's system through the C2 server such as domain name, IP address or which antivirus products or other security solutions are installed on the system (Liska & Gallo, 2017; Belcic, 2020). With this information, the attacker will be able to detect the identity and the value of the victim. Also, to seek for credentials stored on disk or in memory to access privileged accounts to expand the attack (Goody et al., 2020).

This stage is also known as lateral movement and it was most commonly accomplished through the usage of valid credentials in combination with Cobalt Strike beacon, SMB and RDP or through the usage of the same backdoors used to establish a foothold in target's network (Crowdstrike, 2020; Goody et al., 2020). The aim of these types of ransomware is to stay undetected. This is mainly achieved through obtaining root privileges of a system to disable security software (TrendMicro, 2020). To establish persistence and to disable infrastructure that could permit system recovery, the advanced ransomware attack includes a stage wherein a fileless backdoor, such as through a beacon, is installed on the system. Fileless means that the malware, ransomware or encrypted backdoor is only present in the target's memory instead of on the drive to avoid detection as the fileless malware does not leave any footprints for antivirus products to detect (Krishna, 2020). Further explained by respondent 1, fileless means that the malware uses legitimate functionalities of a computer, such as PowerShell on a Windows machine, to life-of-the-land. Shortly said, it uses what is already on the computer instead of creating files. Netwalker is such a fileless ransomware (Victor, 2020).

Furthermore, offenders are also putting other technical measure in place to avoid suspicion such a through a deny/allow list of IP addresses. If particular conditions are met, such as if an individual is using a computer instead of another device or if a foreign IP address is used, the individual is forwarded to the genuine website and not to a malicious website. Other individuals, with the required conditions, are then re-routed to the malicious website (Europol, 2020b).

In case of the BazarLoader attack, a process hollowing will be used to inject the BazarBackdoor component into Windows processes to create, as the name reveals, a backdoor. In essence, process hollowing is an exploit whereby the code is removed in an executable file and replaced with malicious code (ATT&CK MITRE, 2020). Loaders, like the BazarLoader or TrickBot, are an essential part of malware and ransomware attacks as they start the infection chain by distributing the payload (CISA, 2020; Marshanski & Kremez, 2020). The attacker deploys and executes the backdoor from the C2 server where he then installs it on the target's system (CISA, 2020; Marshanski & Kremez, 2020). Every time the user logs into the compromised system, a scheduled task is created to load BazarLoader. After that, BazarBackdoor will deploy a Cobalt Strike beacon, which provides remote access to the attacker (Goody, Kennelly, Shilko, Elovitz & Bienstock, 2020). Through this, the attacker will be able to install exploitation tools such as BloodHound and LaZagne for, among others, extracting credentials (Kremez, 2020). BazarLoader is typically used to move laterally on the network (Hornetsecurity, 2020). In chapter 4.1.2, it was discussed that BazarLoader is a fairly new tool which was first seen during the pandemic and it is uncertain if this is a coincidence. There has not been any evidence that BazarLoader was developed specifically for pandemic-related ransomware attacks. To add to that, the increasingly professionalization of ransomware gangs might explain this.

In the conversation with respondent 1, it was mentioned that ransomware attacks have become more sophisticated since a few years because there is an incentive to be quiet as they eventually do want to get payed. By being noisy, it is easier to detect the offenders and try to avoid damage. To the question what sophisticated means according to him, he answered: “there is no universal definition for a ‘sophisticated’ or say ‘advanced’ attack. Typically, an assessment of a threat actor considered to be sophisticated, particular to cybercrime is heavily influenced by assessing financial impact, geographical scope, level of organization. With that being said, I would classify the threat actor(s) behind Ryuk to be a sophisticated threat actor with access to significant skills or tooling, or with ability to gain entry to a restricted system (e.g., well-resourced cybercriminal threat actor with access to bespoke malware). REvil and Maze are less sophisticated because they have comparably limited resources and sophistication in in-house tooling and techniques, while still posing a substantial threat to organizations. Threat actors can become more sophisticated over time depending on acquisition of new resources (e.g., talent, tools and money)”. Respondent 2 and 3 added that ransomware gangs are increasingly professionalizing throughout the years.

The stage of exploring and expanding was not always found to be part of a ransomware attack targeting the healthcare sector during the pandemic. Some attacks were characterized by simplicity such as the EDA2 ransomware and did not include such a stage. This sometimes depends on the type of scheme used by the offenders, as explained by respondent 1. There are different ransomware schemes: a private scheme whereby the offenders created and deployed the ransomware themselves, a RaaS scheme where the ransomware has been created by someone who is selling it as a service, and there are also schemes wherein the ransomware is leased. The latter means that the creator does not distribute the source code to the other party. A private scheme is often more sophisticated because the creators manage the entire operation themselves, perform reconnaissance and execute it according to their own wishes.

Before the COVID-19 pandemic, offenders have also been using sophisticated techniques to deploy ransomware (Liska, & Gallo, 2017; Microsoft, 2018; Europol, 2020b), and the most well-known example is the WannaCry ransomware. WannaCry was also a sophisticated attack which used fileless techniques to avoid detection (Microsoft, 2018). In addition, as mentioned by respondent 1, the offenders behind the Ryuk ransomware are also pretty sophisticated as they go after the files that hurt the target. For instance, they go after domain controllers, Active Directories or even target the virtual machines that keep the backups. As also mentioned in paragraph 4.1.3, by respondent 1, the hunt on the Ryuk gang is “a sort of big-game hunting” due to the damage they cause. Furthermore, in 2017, Chadha and

Kumar (2017) wrote that ransomware attacks have become more sophisticated by referring to the CryPy ransomware as an example. Thus, even before the pandemic, the sophistication of ransomware attacks was discussed by security professionals and scholars as a trend in the modus operandi. This may be interpreted as a logical trend as offenders will continue to look for ways and take opportunities to outsmart the other, rather than a sudden occasion due to the pandemic.

4.5. The encrypting files, directories or systems stage

The main purpose of this stage is to encrypt the target's files, directories or systems. How this is accomplished, and which cryptographic algorithms are used vary amongst ransomware families (personal communication, respondent 1, December 9, 2020). For instance, the EDA2 ransomware binary works as follows: after the C2 server successfully receives the details, it then creates an encryption key based on the received details and sends the key back to the infected client. Once the key is received from the C2 server, the infected client then initiates another HTTP POST request containing the hostname and main decryption key for the client (McCabe, Ray & Cortes, 2020).

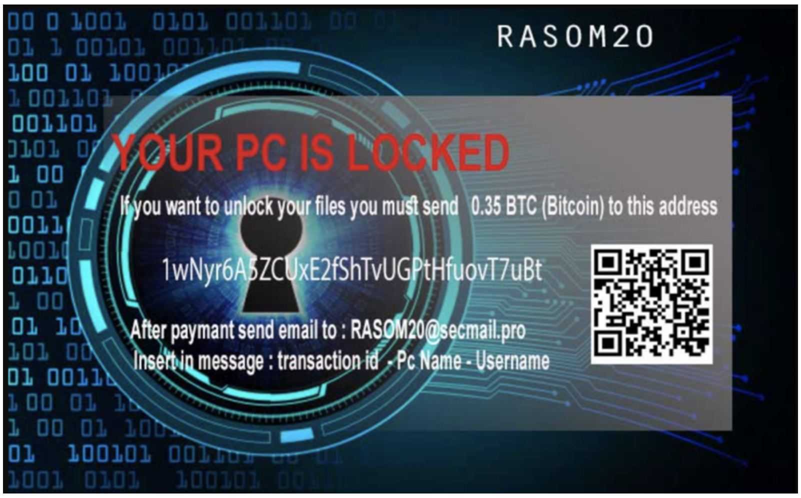
Additionally, EDA2 uses a quite simple cryptographic algorithm whilst Ryuk ransomware has used a combination of symmetric and asymmetric encryption through using AES-256 and RSA-2048 to encrypt files and an RSA public key to encrypt the AES key (CISA, 2020; McCabe, Ray & Cortes, 2020; personal communication, respondent 1, December 9, 2020). The most common situation is the encryption of files, such as PDF or Office-documents on a personal laptop or computer, this was also confirmed by both respondent 1 and 2.

The particular ransomware binary is configured to encrypt files with the file extensions as determined by the attacker via the C2 processes. For instance, the Netwalker ransomware mainly target common user files such as Office documents, PDFs, images, videos, and text files (Victor, 2020). Some ransomware binaries, such as EDA2, have a limitation. EDA2 only encrypts files and directories that are on the victim's desktop (McCabe, Ray & Cortes, 2020), wherein other ransomware binaries also encrypt the filenames, making it even more difficult to identify how far the offenders have gotten and which particular files are gone (Liska, & Gallo, 2017). Moreover, sometimes offenders were getting sloppy or realized they were caught, and basically encrypted everything they can to still make the best out of it, as described by respondent 1.

The encryption stage is a crucial characteristic of a ransomware attack. If files, directories or systems are not encrypted, the offenders lack having an effective extortion method. Offenders can pretend to have encrypted files to force the victim in paying money, however this is called scareware instead of ransomware (Crowdstrike, 2019; Cybereason, 2020). More specifically, as mentioned in chapter two, ransomware is "software designed by criminals to prevent computer users from getting access to their own computer system or files unless they pay money" (Cambridge Dictionary, "ransomware", n.d.). Thus, cryptography is used as a primary extortion method for demanding money. The next stage will elaborate on this in more detail. Moreover, ever since ransomware exist, algorithms used to encrypt files vary amongst ransomware families; some only use symmetric or asymmetric key encryption, others combine these two (Liska & Gallo, 2017; personal communication, respondent 1, December 9, 2020). The pandemic did not influence this part of the modus operandi. As criminals are becoming smarter, they are looking for ways to use more sophisticated encryption techniques making it more difficult to decrypt for the other party. Hence, this indicates that the COVID-19 pandemic has not affected this step of the crime-commission process.

4.6. The extortion and monetization stage

The last stage of the crime-commission process is the extortion and monetization stage. Once the selected files or directories have been encrypted through the C2 processes, a message will appear on the victim's screen stating that his system has been compromised and their files or directories are encrypted. Through this, the offenders extort the victim to pay a ransom. Typically, an image will be saved on the C drive and displayed to the user through the user's desktop wallpaper (Belcic, 2020; McCabe, Ray & Cortes, 2020), or a text-file will be saved on the victim's computer which includes a clear instruction on how to pay the ransom (personal communication, respondent 1, December 9, 2020). Picture 1 presented an example of such an image.



RASOM20

YOUR PC IS LOCKED

If you want to unlock your files you must send 0.35 BTC (Bitcoin) to this address

1wNyr6A5ZCUxE2fShTvUGPtHfuovT7uBt

After paymant send email to : RASOM20@secmail.pro
Insert in message : transaction id - Pc Name - Username

Picture 1. Adapted from “Malicious Offenders Target Government and Medical Organizations With COVID-19 Themed Phishing Campaigns,” by McCabe, A., Ray, V., & Cortes, J., 2020, retrieved from https://unit42.paloaltonetworks.

Ransom notes are often quite generic, as explained by respondent 1, and comparable amongst ransomware families. Included in the message is the amount to be paid to regain access to the files, directories or system and in some cases a timer that shows how long before they will increase the price, or the files will become unrecoverable (Meskauskas, 2020). In some cases, such as at the Ryuk attack, a communication channel between the victim and attacker was established by using an end-to-end encrypted email provider (CISA, 2020; (McCabe, Ray & Cortes, 2020). By this mean, the victim could contact the attacker (Europol, 2020b). Through the message displayed on the screen, the victim receives instructions to contact the attacker.

After the victim contacts the attacker, the ransom amount will be announced, and the victim is told to pay the designated ransom amount to a specified crypto wallet (CISA, 2020; McCabe, Ray & Cortes, 2020). As further explained by respondent 1, offenders more often choose the method of including a private centric email instructing the victim to send an email to that particular address with the digits presented in the ransom note instead of including a crypto wallet address in the note. Offenders choose this method for operational security and secrecy purposes. Lastly, another method of extortion used by some ransomware families is through an audio message as part of the ransom note that addresses the victim aloud (Belcic, 2020). The audio contained, among other things, clear instructions on how and when to pay the ransom.

Offenders also pressure victims to pay the ransom by extracting their data and threatening to publish it (Europol, 2020b). Once offenders gain a foothold on the network, they explore the network and exfiltrate sensitive data. If the victim refuses to pay the ransom, offenders will publish the data or sell it to the highest bidder. By this means, threatening to publish the stolen data in combination with encrypting the data works as a double extortion method, as explained by respondent 1 and 2. This was also the case at the Affordacare urgent care clinic in Texas whereby offenders, during the pandemic, eventually published the stolen data after the clinic refused to pay the ransom (DataBreaches.net, 2020). Moreover, as stated by Passeri (2020), "with double extortion attacks, even if a backup is available the offenders can put more pressure on the victim to pay the ransom. The increased pressure comes from the potential serious consequences of a data leak, for example economic and reputational damage". This, however, is not a novel tactic as it was already used in 2019 by the Maze ransomware gang (Heller, 2019). For instance, in November 2019, the gang leaked nearly 700 MB of files stolen from Allied Universal in a ransomware attack because they did not pay the ransom on time (Heller, 2019).

There were also ransomware families, such as Ryuk, where they offered support to their victims through some sort of a support desk, this was also confirmed by all respondents in the interviews. By this means, it was possible to chat with the offenders through the support desk, and some families even offered the victims support for a maximum of 72 hours. Even though this is a remarkable technique and, according to respondent 1, it has become especially prevalent this year since most are following the same model and ransomware victims have increased, it has been around for a while, even before the pandemic (Finkle, 2016).

The ransom amount varies amongst ransomware families and even attacks, from hundreds of thousands to millions of dollars. Some families did some sort of reconnaissance to identify the value of the victim and based on the information, the ransom was determined. In all the cases, payment was demanded in cryptocurrencies because those transactions are harder to trace (Petters, 2020). Bitcoins and other cryptocurrencies are nowadays the preferred way of obtaining money from the victims and this has not changed since COVID-19. Other payment methods used to be through SMS text messages or by mailing pre-paid cards (Richardson & North, 2017) but this changed in 2008 when Bitcoin was introduced (Conti, Gangwal & Ruj, 2018). The previous ransomware payment methods were too risky as it was possible to follow the money that leads to the attacker. Cryptocurrencies are less risky because it is much harder to trace the transactions and therefore difficult or even impossible to identify the attacker (Richardson & North, 2017; Conti, Gangwal & Ruj, 2018; Paquet-Clouston, Haslhofer & Dupont, 2019). Ever since cryptocurrencies came into the picture, ransomware attacks grew, and offenders favor this ransomware payment method as the default method (Richardson & North, 2017; Conti, Gangwal & Ruj, 2018; Paquet-Clouston, Haslhofer & Dupont, 2019; Europol, 2020b).

After the ransom was paid by the victims, the decryptor, which is a tool to recover the encrypted files, and a sample decryption of some files will be provided to the victim (CISA, 2020; McCabe, Ray & Cortes, 2020). According to the respondents, most of the time the files were eventually decrypted. In some cases, due to technological issues, it was not possible to decrypt the files. However, as explained by respondent 1, offenders have a reputation which they would like to maintain because if people know that files are not decrypted after paying the ransom, it is less likely that victims will pay the ransom. Thus, there is an incentive for offenders to actually follow through and decrypt the files. This would also explain the support the offenders provide to their victims to ensure that victims are paying the ransom and files are decrypted.

Again, the question is, has this changed since COVID-19 or did this part of the modus operandi exist before the pandemic? First and foremost, the purpose of ransomware is monetary gain and offenders are financially motivated, as stated by the respondents. To be able to get the money, the offenders will have to find a way to put some pressure on the victims, otherwise there will be no incentive for the victims to pay the ransom. Additionally, offenders foster their own reputation by ensuring that the files will be decrypted after the ransom has been payed. Hence, offenders will do anything to make sure that they receive the money and so, it is within the nature of the phenomenon itself that ransomware attacks include a step within its crime-commission, and thus the modus operandi, wherein victims are extorted for monetary gain. This makes it highly unlikely that the pandemic has changed or even will change this. Secondly, there were no new ways of extorting the victim identified, neither new ways of monetization during the pandemic.

4.7. A changed modus operandi?

By aggregating the foregoing information and looking back at the results, the interview participants were asked about their perspectives on the impact of the pandemic on the modus operandi. None of the participants think that the pandemic has caused cybercriminals to change their modus operandi. They all agree that the pandemic is just another opportunity for cybercriminals to commit a crime and nothing more.

5. Conclusion and discussion

The aim of this research was to identify to what extent the COVID-19 pandemic changed the modus operandi of offenders to commit a ransomware attack targeting the healthcare sector. In order to research this, firstly a crime script was established to shed a light on the crime-commission process by breaking this up in smaller pieces. The established crime script formed the foundation of the analysis on whether the pandemic influenced the modus operandi of a ransomware attack. This was accomplished through the identified six stages and a review of literature, documents and reports. Additionally, interviews were held for validity purposes. In summary, the analysis of various sources and data from interviews showed that the COVID-19 pandemic slightly changes the modus operandi, with only a minor change in the approach to lure the victims. No significant changes in the modus operandi were identified.

Through the establishment of the theoretical framework, we learned that criminals are typically opportunistic. Following the crime opportunity theory, the routine activity theory and situational factors, a ransomware attack towards the healthcare sector is certainly not a surprise given the crucial nature of this sector. Furthermore, by demonstrating how these attacks take place through the established crime script, it is possible to identify the modus operandi and opportunities misused by offenders during the pandemic. The crime script contained six stages, namely: 1) preparation, 2) initial access and compromise, 3) command-and-control, 4) exploring and expanding, 5) encrypting files, directories or systems, and 6) extortion and monetization.

During the preparation stage, offenders will typically determine which ransomware family, methods and tools are used to conduct the attack. Similarly, it was investigated that an important element of a ransomware attack is to establish a C2 communication channel and the establishment of a C2 communication channel requires a domain name. Amongst other things, various reports have claimed that COVID-19-related domain names are more likely to be malicious than other registered domain names. Following the crime opportunity theory and considering the situational factors, an increase in newly COVID-19 registered malicious domain names is not astonishing. Though, the results showed those reports are quite contradictory and mostly incomplete. As such, more quantitative research is required to determine whether there truly is a significant relationship between COVID-19 and newly registered malicious domain names to assess whether this actually poses a problem.

Furthermore, it was investigated whether new tools or ransomware families were used during the pandemic. To conclude, offenders mostly used already existing tools and ransomware families in their attacks on the healthcare sector. The tool BazarLoader and the family Egregor were the only exceptions. Whether or not it is a coincidence that BazarLoader and Egregor showed up during the pandemic is not clear. It requires additional research to determine whether there is a relationship between the release of BazarLoader and Egregor, and the COVID-19 pandemic. Mainly because of the increase in the sophistication of attacks and the continuous evolvement of ransomware families through the deployment of new features or emergence of new families. Technology is evolving quickly, and offenders always look for a way to evade detection. Importantly, it appears that there was already an upwards trend in RaaS schemes which makes it unlikely that the pandemic has led to the development of the new RaaS-schemed family, Egregor. Nonetheless, the lack of evidence has led to the conclusion that the pandemic did not affect the modus operandi. Additional research will have to indicate whether there is a causal relationship.

Through analyzing the available data, three ways of gaining initial access and deploying ransomware were identified: through phishing emails, a brute force attack or the exploitation of internet-exposed services and public-facing applications. Various reports have revealed that a phishing attack was the most common used method of gaining initial access to a system during the pandemic. Before the pandemic, gaining access to a system was also mostly accomplished through phishing mails as this was the preferred method used by offenders. Thus, the study has clarified that the modus operandi did not change.

Additionally, it was discussed that offenders misused the pandemic to increase urgency by including words related to COVID-19. However, knowing that crime is typically opportunistic, COVID-19 related keywords may as well be replaced by other keywords related to another disaster or event. This has led to the conclusion that the COVID-19 crisis is no difference to this end. When considering this, it became apparent that the modus operandi slightly changed because offenders adjusted their method to lurk victims. Even though it does not entail a major change, it does fuel the debate that crime follows opportunities as explained in the theoretical framework. Also, it turned out that reports often cite that offenders misuse the pandemic by misleading victims via phishing emails containing COVID-19 related keywords. The minor change in the modus operandi can be explained through the crime opportunity theory and situational factors. Following these theories, it appears that these developments seem to form a trend pattern. This ties in with Cohen's perspective and statement "opportunity makes the thief". These events should therefore be looked at from this perspective to avoid moral panic. Statements from intergovernmental institutions should take this into account as it can happen in any crisis or even event.

Furthermore, it was investigated that the second way of gaining initial access, through a brute-force attack towards RDP, is not a new phenomenon. It was concluded that there has been an increase in RDP-related attacks during the pandemic which indicates that the lockdown has a significant effect on the number of RDP-related attacks, such as brute-force attacks. However, it will have to be further investigated whether this is actually the case by increasing the scope and looking at changes compared to one or two years ago. The results also showed that the exploitation of internet-exposed services and public-facing applications is again something we have seen before. As such, both methods of gaining initial access are not a new in terms of the modus operandi. This leads to the conclusion that the pandemic did not change the modus operandi in this regard.

However, as already discussed, RDP-related attacks which also include the exploitation of RDP or SMB related vulnerabilities, are on the rise. In summary, it can be concluded that the rise in people working from home since the pandemic has led to an increase in the attack surface on RDP-related attacks, both through exploiting vulnerabilities and brute-force attacks as it has opened up more opportunities. Consequently, the increase in RDP-related attacks can be explained through the crime opportunity theory as the pandemic triggered a rise in people working remotely, but also through the lens of the routine activity theory. The increase in working remotely provides more suitable targets, often with an insecure network. Even though the focus of this study is to discover changes in the modus operandi and not to identify change in the extent, this observation is worth mentioning as it can be valuable in terms of further scientific research.

It was discussed that the command-and-control stage is an indispensable step in the crime-commission process of a ransomware attack and it has been around for a while. This study has clarified that no changes were identified in the modus operandi. This part of the modus operandi may not be interpreted as a new opportunity but rather as a crucial component to deploy a successful ransomware attack. This applies to any ransomware attack, not only during the pandemic at the healthcare sector.

Furthermore, the stage 'exploring and expanding' was not always found to be part of an attack but in most of the cases it was. Throughout the years, offenders have also been using sophisticated techniques to deploy ransomware, not only during the pandemic. It was concluded that this stage is not a new part of the modus operandi, but it rather may be interpreted as a logical trend as offenders will continue to look for ways and take opportunities to outsmart the other, rather than a sudden occasion due to the pandemic. It appears that the COVID-19 pandemic did not change the modus operandi to this end.

A fifth stage was identified wherein the attacker encrypts the victim's files, directories or systems. Similar to the command-and-control stage, it appears that this stage is a crucial characteristic of a ransomware attack. As criminals are becoming smarter, they are looking for ways to use more sophisticated encryption techniques making it more difficult to decrypt for the other party. Consequently, it became apparent that the COVID-19 pandemic has not affected this step of the modus operandi.

The last stage of the crime-commission process is the extortion and monetization stage. It was also discussed that offenders have a reputation, which provides an incentive to decrypt the files after the ransom has been paid by the victim. Another method is through double extortion, whereby offenders pressure victims to pay the ransom by extracting their data and threatening to publish it. None of the methods had been identified as 'new' because these methods were already used before the pandemic by offenders. This also applies to monetization as criminals have favored cryptocurrencies for a while now due to its anonymity. Again, there is no indication of a change in modus operandi due to the pandemic.

Hence, it became clear that none of the participants think that the pandemic has caused cybercriminals to change their modus operandi. They all agreed that the pandemic is just another opportunity for cybercriminals to commit a crime and nothing more.

Taking this together, the results of this study indicate that the modus operandi differs just a slightly bit from the situation before the COVID-19 pandemic. The only change is the method of deceiving victims by luring them through phishing mails with COVID-19 related keywords. However, this may not be interpreted as a significant change in the modus operandi as it only provides additional options to lure the victims. Also, knowing that crime is typically opportunistic, COVID-19 related keywords may as well be replaced by other keywords related to another disaster.

It seems like that the pandemic has not brought about major changes in cybercriminals' modus operandi, nor has it created many new opportunities. The opportunities as identified in this research are in line with the theories as presented in the theoretical framework. This indicates that most of the claims stating that COVID-19 has caused a serious change in ransomware attacks on the healthcare sector and that this has opened up new opportunities for criminals, are somewhat exaggerated by intergovernmental institutions and causing moral panic. This could eventually lead to disproportionate response. However, this does not mean that nothing should be done about the information security posture of the healthcare sector as they remain a vulnerable sector for ransomware attacks. On the other hand, it does mean that we must remain critical in circumstances where others argue that cyber security is at stake due to a particular event. The dynamic environment in which cybercriminals operate and the opportunities they will exploit at all times must be taken into account.

6. Recommendations

The recommendations of this research are two folded: firstly, practical recommendations for the healthcare sector to help them gain resilience for future ransomware attacks are provided, and secondly, recommendations for intergovernmental institutions to have a more critical perspective on both the current as well as future events are provided.

This research has shed a light on the poor security of hospitals. With the acquired knowledge of the opportunities through the crime script analysis and the vulnerabilities of hospitals, we can translate these findings to practical recommendations for the healthcare sector to help them gain resilience for future ransomware attacks. Knowing that a crisis is inevitable, it is first and most forward important to establish a crisis management team with the essential competences. Such a team will be able to identify the early signs of a crisis, the problem areas and determine what is necessary to protect the organization.

Furthermore, the team should also focus on communication towards the healthcare organization's employees. Through communicating, the crisis management team can warn the employees for what might come in order to prepare themselves and be more aware. Awareness is one of the key aspects, as most of the systems have been compromised through phishing attacks. This was indicated by the crime script analysis. As such, healthcare organizations should enforce its employees to participate in a security awareness program in order to foster a secure culture. Employees should be trained to recognize a malicious email, attachment and URL, and they should be aware of the organization's incident management procedure.

Additionally, the increase in working remotely provides more suitable targets, often with an insecure network. It became appeared that hospitals are often left vulnerable with an inefficient patch management process. It is important to keep in mind that hospitals were already vulnerable before the pandemic. It is nevertheless important to inform hospitals, the broader healthcare sector and policymakers of the usefulness of, amongst others, patch management. As such, healthcare organizations should implement a patch management policy to prevent that systems are not patched regularly or timely. Unpatched systems can lead to offenders exploiting the vulnerabilities to compromise the system.

Also, an identity and access management policy should ensure that the need-to-know principle is enforced by only allocating access rights to systems or applications to those who need it to do their job. If less employees have privileged access, it is most difficult for the attacker to obtain credentials of a privileged account. This, in combination with a strict password policy including multi-factor authentication, makes it harder for offenders to either gain initial access or to expand the attack. Lastly, hardening policy should prevent systems to be misconfigured and therefore vulnerable for attacks. An RDP-related attack will be less likely if the RDP is configured appropriately.

The results indicate that most of the claims stating that COVID-19 has caused a serious change in ransomware attacks on the healthcare sector and that this has opened up new opportunities for criminals or changed the modus operandi, are exaggerated by intergovernmental institutions and leading to moral panic. This could eventually lead to disproportionate response. Especially taking into consideration that ransomware during the pandemic is a trend pattern and just another opportunity for offenders to commit cybercrime. As such, it is recommended to have a more critical look on the events and the data by conducting further scientific research. An important prerequisite is the researcher's independence because reports from, for example, security providers are questionable due to their commercial interests. Lastly, sufficient data should be collected from a reasonable longer period before the pandemic in order to increase validity.

7. References

Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society, 32(3),* 183-196. doi: 10.1016/j.techsoc.2010.07.001

Abrams, L. (2020). SunCrypt ransomware sheds light on the Maze ransomware cartel. Retrieved on 12 December 2020 from <https://www.bleepingcomputer.com/news/security/suncrypt-ransomware-sheds-light-on-the-maze-ransomware-cartel/>

Advanced Intel. (2020). NetWalker ransomware group enters advanced targeting “game”. Retrieved on 14 November 2020 from <https://www.advanced-intel.com/post/netwalker-ransomware-group-enters-advanced-targeting-game>

Acronis. (n.d.). The NHS cyber attack. Retrieved on 6 December 2020 from <https://www.acronis.com/en-eu/articles/nhs-cyber-attack/#:~:text=The%20WannaCry%20ransomware%20exposed%20a,extremities%20of%20the%20cyber%2Dattack.>

Ashby, M. P. J. (2016). Is metal theft committed by organized crime groups, and why does it matter? *Criminology and Criminal Justice, 16(2),* pp. 141–157.

ATT&CK MITRE. (2020). Process injection: process hollowing. Retrieved on 15 November 2020 from <https://attack.mitre.org/techniques/T1055/012/>

Belcic, I. (2020). Cerber Ransomware: everything you need to know. Retrieved on 6 December 2020 from <https://www.avast.com/c-cerber>

Bertram, A. (2019). How offenders use BloodHound to get Active Directory domain admin access. Retrieved on 6 December 2020 from <https://mcpmag.com/articles/2019/11/13/bloodhound-active-directory-domain-admin.aspx>

Boddy, A., Hurst, W., Mackay, M., & El Rhalibi, A. (2017). A study into data analysis and visualisation to increase the cyber resilience of healthcare infrastructures. *IML '17: Proceedings of the 1st International Conference on Internet of Things and Machine Learning, 32*, pp. 1-7.

Boin, A., & McConnell, A. (2007). Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience. *Journal of Contingencies and Crisis Management, 15(1),* pp. 50-59.

Bossler, A. M., & Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice, 38(3),* 227-236. doi: 10.1016/j.jcrimjus.2010.03.001

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9(2),* pp. 27-40.

Buchanan, B. (2017). The legend of sophistication in cyber operations. Retrieved on 5 December 2020 from <https://www.belfercenter.org/publication/legend-sophistication-cyber-operations>

Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. H. (2015). The persuasion and security awareness experiment: reducing the success of social engineering attacks. *Journal of Experimental Criminology, 11(1),* 97-115. doi: 10.1007/s11292-014-9222-7

Buyens, K., De Win, B., & Joosen, W., (2007). Empirical and statistical analysis of risk analysis- driven techniques for threat management. The Second International Conference on Availability, Reliability and Security (ARES'07). doi: 10.1109/ARES.2007.78

CENTR.org. (2020). The true effect of corona on the DNS. Retrieved on 5 November 2020 from <https://centr.org/news/blog/the-true-effect-of-corona-on-the-dns.html>

Chadha, S., & Kumar, U. (2017). Ransomware: let's fight back! *International Conference on Computing, Communication and Automation (ICCCA2017),* pp. 925-930. doi:10.1109/ccaa.2017.8229926

Check Point. (n.d.). COVID-19 impact: as retailers close their doors, hackers open for business. Retrieved on 28 November 2020 from <https://blog.checkpoint.com/2020/03/19/covid-19-impact-as-retailers-close-their-doors-hackers-open-for-business/>

Chiew, K. L., Yong, K. S. C. & Tan, C. L. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Systems with Applications, 106,* pp. 1-20. doi: 10.1016/j.eswa.2018.03.050

Clough, J. (2015). *Principles of cybercrime.* Cambridge: Cambridge University Press. doi: 10.1017/CBO9781139540803

CobaltStrike. (2012). Meet Cobalt Strike: Adaptive Pen Testing. Retrieved on 6 December

2020 from <https://blog.cobaltstrike.com/2012/06/14/meet-cobalt-strike-adaptive-pen-testing/ >

Cohen, L. E. (1981). Modeling crime trends: A criminal opportunity perspective. *Journal of Research in Crime & Delinquency, 18(1*), pp. 138-164.

Cohen, L. E. & Felson, M. (1979). Social change and crime rate trends: a routine activity approach. American Sociological Review, 44(4), pp. 588-608.

Conti, M., Gangwal, A., & Ruj, S. (2018). On the economic significance of ransomware campaigns: A Bitcoin transactions perspective. *Computers & Security, 79,* pp. 162-189. doi: 10.1016/j.cose.2018.08.008

Cornish, D. (1994). The procedural analysis of offending and its relevance for situational prevention. *Crime Prevention Studies, 3,* pp. 151–196.

Crowdstrike. (2019). What is ransomware? Retrieved on 13 November 2020 from <https://www.crowdstrike.com/epp-101/what-is-ransomware/>

Crowdstrike. (2020). Threat hunting uncovers more intrusions against healthcare in midst of COVID-19 pandemic. Retrieved on 13 November 2020 from <https://www.crowdstrike.com/blog/how-threat-hunting-uncovers-covid-19-healthcare-attacks/>

Cybersecurity and Infrastructure Security Agency (CISA). (2020). Alert (AA20-302A) Ransomware activity targeting the healthcare and public health sector. Retrieved on 30 October 2020 from <https://us-cert.cisa.gov/ncas/alerts/aa20-302a>

Cybereason. (2020). Just because you're home doesn't mean you're safe. Retrieved on 3 November 2020 from <https://www.cybereason.com/blog/just-because-youre-home-doesnt-mean-youre-safe>

Cyware. (2020). Links discovered between Bazar and TrickBot. Retrieved on 27 November 2020 from <https://cyware.com/news/links-discovered-between-bazar-and-trickbot-2909546d>

DataBreaches.net. (2020). Urgent care walk-in centers in Texas and Florida suffer cyberattacks. Retrieved on 5 December 2020 from <https://www.databreaches.net/urgent-care-walk-in-centers-in-texas-and-florida-suffer-cyberattacks/>

Davinson, N., & Sillence, E. (2010). It won't happen to me: promoting secure behaviour among internet users. *Computers in Human behavior, 26(6),* 1739-1747. doi: 10.1016/j.chb.2010.06.023

Davis, J. (2020). ASPR warns ransomware threat is persistent, as actors leak more data. Retrieved on 11 December 2020 from <https://healthitsecurity.com/news/aspr-warns-ransomware-threat-is-persistent-as-actors-leak-more-data>

Dehghanniri, H., & Borrion, H. (2016). Toward a more structured crime scripting method. *2016 IEEE 24th International Requirements Engineering Conference Workshops,* pp. 94-98. doi: 10.1109/REW.2016.030

Dehghanniri, H., & Borrion, H. (2019). Crime scripting: A systematic review. *European Journal of Criminology, 00(0),* pp. 1-2. doi: 10.1177/1477370819850943

Demuro, P. R. (2017). Keeping internet pirates at bay: ransomware negotiation in the healthcare industry. Nova Law Review, 40, pp. 349-396.

Dredge, S. (2014). Ebola advice emails from 'World Health Organization' are malware spam. Retrieved on 20 June 2020 from <https://www.theguardian.com/technology/2014/oct/23/ebola-malware-spam-email-world-health-organization>

Ducharme, J. (2020). World Health Organization declares COVID-19 a 'pandemic.' Here's what that means. Retrieved on 23 August 2020 from <https://time.com/5791661/who-coronavirus-pandemic-declaration/>

Europol. (2016). Ransomware: what you need to know - a joint report by Check Point and Europol. Retrieved on 28 November 2020 from <https://www.cyberwiser.eu/system/files/ransomware-what_you_need_to_know_1.pdf>

Europol. (2020a). Beyond the pandemic how COVID-19 will shape the serious and organised crime landscape in the EU. Retrieved on 8 June 2020 from: <https://www.europol.europa.eu/activities-services/staying-safe-during-covid-19-what-you-need-to-know>

Europol. (2020b). Internet organised crime threat assessment. Retrieved on 5 December 2020 from <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020>

Finkle, J. (2016). Ransomware: Extortionist hackers borrow customer-service tactics.

Retrieved on 18 December 2020 from < https://www.reuters.com/article/us-usa-cyber-ransomware-idUSKCN0X917X>

Furnell, S., Emm, D., & Papadaki, M. (2015). The challenge of measuring cyber-dependent crimes. *Computer Fraud & Security, 10, pp. 5-12.* doi: 10.1016/S1361-3723(15)30093-2

Frank, D., Zhao, M., & Dahan, A. (2020). A Bazar of Tricks: following team9's development cycles. Retrieved on 13 November 2020 from <https://www.cybereason.com/blog/a-bazar-of-tricks-following-team9s-development-cycles>

Galletta, A., & William, E. C. (2013). *Mastering the semi-structured interview and beyond: from research design to analysis and publication.* New York: NYU Press.

GitHub. (n.d. a). BloodHoundAD/BloodHound. Retrieved on 6 December 2020 from <https://github.com/BloodHoundAD/BloodHound>

GitHub. (n.d. b). AlessandroZ/LaZagne. Retrieved on 6 December 2020 from <https://github.com/AlessandroZ/LaZagne

GitHub. (n.d. c). EmpireProject/Empire. Retrieved on 6 December 2020 from <https://github.com/EmpireProject/Empire>

Gittins, Z., & Soltys, M. (2020). Malware persistence mechanisms. *Procedia Computer Science, 176,* pp. 88-97. doi: 10.1016/j.procs.2020.08.010

Goody, K., Kennelly, J., Shilko, J., Elovitz, S., & Bienstock, D. (2020). Threat research – Unhappy hour special: KEGTAP and SINGLEMALT with a ransomware chaser. Retrieved on 13 November 2020 from <https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html>

Gordon, S. & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology, 2(1),* pp. 13-20. doi: 10.1007/s11416-006-0015-z

Gostev, A., Zaitsev, O., Golovanov, S., & Kamluk, V. (2008). Kaspersky Security Bulletin Malware evolution 2008. Retrieved on 28 November 2020 from <https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/20140350/kaspersky_security_bulletin_part_1_threats_en.pdf>

Greenberg, A. (2008). Economic Bust, Cybercrime Boom. Retrieved on 20 June 2020 from <https://www.forbes.com/2008/11/18/cybercrime-boom-fraud-tech-security-cx_ag_1119crime.html>

Gregory, P. H. (2018). *CISM – certified information security manager all-in-one exam guide.* New York: McGraw-Hill Education.

Grober, D. (2020). Roundup: COVID-19 pandemic delivers extraordinary array of cybersecurity challenges. Retrieved on 18 December 2020 from <https://www.zdnet.com/article/roundup-the-coronavirus-pandemic-delivers-an-array-of-cyber-security-challenges/>

Guerra, P. (2009). How economics and information security affects cyber crime and what it means in the context of a global recession. Retrieved on 20 June 2020 from <https://www.blackhat.com/presentations/bh-usa-09/GUERRA/BHUSA09-Guerra-EconomicsCyberCrime-PAPER.pdf>

Gujraniya, D., Waseem, M., Ar, B., & Singh, S. (2018). Ransomware command and control detection using machine learning. Retrieved on 6 December 2020 from <https://www.acalvio.com/ransomware-command-and-control-detection-using-machine-learning/#:~:text=To%20encrypt%20machine's%20data%2C%20ransomware,for%20all%20the%20infected%20hosts.>

Hall, G. E. (2020). Remove BazarLoader malware (removal guide) - free instructions. Retrieved on 27 November 2020 from <https://www.2-spyware.com/remove-bazarloader-malware.html>

Hanel, A. (2019). Big game hunting with Ryuk: another lucrative targeted ransomware. Retrieved on 30 October from <https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/>

Harkins, M., & Freed, A. M. (2018). The ransomware assault on the healthcare sector. *Journal of Law and Cyber Warfare, 6(2),* pp. 148-164.

Heller, M. (2019). Maze gang outs ransomware victims in shame campaign. Retrieved on 13 December 2020 from <https://searchsecurity.techtarget.com/news/252475664/Maze-gang-outs-ransomware-victims-in-shame-campaign?_ga=2.178581028.1440348712.1607875185-544356748.1607875185>

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. Deviant Behavior, 30(1), 1–25. doi: 10.1080/01639620701876577

Holt, T. J., Van Wilsem, J., Van De Weijer, S., & Leukfeldt, R. (2020). Testing an integrated self-control and routine activities framework to examine malware infection victimization. Social Science Computer Review, 38(2), 187–206. doi: 10.1177/0894439318805067

Hornetsecurity. (2020). BazarLoader campaign with fake termination emails. Retrieved on 6 December 2020 from <https://www.hornetsecurity.com/en/threat-research/bazarloader-campaign-with-fake-termination-emails/>

Hutchings, A., & Holt, T. J. (2014). A crime script analysis of the online stolen data market. *The British Journal of Criminology, 55(3),* pp. 596–614.

Intel471. (2020). Ransomware-as-a-service: The pandemic within a pandemic. Retrieved on 27 November 2020 from <https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/>

Interpol. (2020). Cybercriminals targeting critical healthcare institutions with ransomware. Retrieved on 16 October 2020 from <https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware>

Ivanov, A. M. (2014). A multiheaded battering ram: RDP Bruteforce attacks on the rise. Retrieved on 29 November 2020 from <https://www.welivesecurity.com/2020/06/29/remote-access-risk-pandemic-cybercrooks-bruteforcing-game/>

Jagatic, T., Johnson, N., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM, 50(10),* pp. 94-100. doi: 1 0.1145/1290958.1290968

Jackson, M. (2005). Law enforcement in cyberspace: The Hong Kong approach. In R. Broadhurst & P. Grabosky (Eds.) *Cyber-crime – The challenge of Asia.* Hong Kong: Hong Kong University Press.

Kaspersky. (2020). How COVID-19 changed the way people work. Retrieved on 29 November 2020 from https://media.kasperskydaily.com/wp-content/uploads/sites/92/2020/05/03191550/6471_COVID-19_WFH_Report_WEB.pdf

Kent, C. (2020). Why are healthcare cyberattacks surging amid Covid-19. Retrieved on 16

October from <https://www.medicaldevice-network.com/features/cyberattacks-healthcare-covid-19/>

KnowBe4. (n.d.). Cerber ransomware. Retrieved on 6 December 2020 from <https://www.knowbe4.com/cerber-ransomware>

KrebsonSecurity. (2018). Who is Agent Tesla? Retrieved on 6 November from <https://krebsonsecurity.com/2018/10/who-is-agent-tesla/>

Krishna, B. L. (2020). Comparative study of fileless ransomware. International Journal of Trend in Scientific Research and Development, 4(3), pp. 608-616.

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care, 25,* pp. 1–10. doi: 10.3233/THC-161263

Kubovič, O. (2020). Remote access at risk: Pandemic pulls more cyber-crooks into the brute-forcing game. Retrieved on 28 November 2020 from <https://www.welivesecurity.com/2020/06/29/remote-access-risk-pandemic-cybercrooks-bruteforcing-game/>

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2020). Cyber security in the age of COVID-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Retrieved on 23 August 2020 from <https://arxiv.org/abs/2006.11929>

Lavorgna, A. (2014). Wildlife trafficking in the Internet age. *Crime Science, 3(5),* pp. 1-12.

Lavorgna, A. (2018a). Analysis and prevention of organised crime. In R. Wortley, A. Sidebottom, N. Tilley & G. Laycock (Eds.) *Routledge Handbook of Crime Science.* London: Routledge.

Lavorgna, A. (2018b). Cyber-organised crime. A case of moral panic? *Trends in Organized Crime, 22,* pp. 357-374.

Leclerc, B. (2017). Crime scripts. In R. Wortley & M. Townsley (Eds.) *Environmental criminology and crime analysis.* London: Routledge.

Lever, R. (2020). Ransomware surge imperils hospitals as pandemic intensifies. Retrieved on 18 December 2020 from <https://techxplore.com/news/2020-11-ransomware-surge-imperils-hospitals-pandemic.html>

Limaye, R. J., Sauer, M., Ali, J., Bernstein, J., Wahl, B., Barnhill, A., & Labrique, A. (2020).

Building trust while influencing online COVID-19 content in the social media world. The Lancet Digital Health, 2 (6), pp. 277-278.

Liska, A. & Gallo, T. (2017). *Ransomware: defending against digital extortion.* Sebastopol: O'Reilly Media Inc.

Lloyd, S. (2020). Reporting potential pandemic-related domains. Retrieved on 5 December 2020 from <https://www.icann.org/news/blog/reporting-potential-pandemic-related-domains>

Lohrmann, D. (2020). 2020: The year the COVID-19 crisis brought a cyber pandemic. Retrieved on 18 December 2020 from <https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-brought-a-cyber-pandemic.html>

Talja, S. (1999). Analyzing qualitative interview data: The discourse analytic method. *Library & Information Science Research, 21(4),* 459-477.

Tcherni, M., Davies, A. L. B., Lopes, G., & Lizotte, A. (2016). The dark figure of online property crime: Is cyberspace hiding a crime wave? *Justice Quarterly, 33(5),* pp. 890-911. doi: 10.1080/07418825.2014.994658.

Thornton, P. M. (2009). Crisis and governance: SARS and the resilience of the Chinese Body Politic. *The China Journal, 61,* pp. 23-48.

TrendMicro. (2016). New open source ransomware based on hidden tear, EDA2. Retrieved on 5 November 2020 from <https://www.trendmicro.com/en_us/research/16/h/new-open-source-ransomwar-based-on-hidden-tear-and-eda2-may-target-businesses.html>

Tuluc, A. M. (2011). The growing global threat of cyber-crime given the current economic crisis: a study regarding Internet malicious activities in Romania. *Acta Universitatis Danubius: Oeconomica., 7(1*), pp. 179-189.

Mahadevan, P. (2020). Cybercrime: Threats during the COVID-19 pandemic. Retrieved on 25 September 2020 from <https://globalinitiative.net/wpcontent/uploads/2020/04/Cybercrime-Threats-during-the-Covid-19-pandemic.pdf>

Mallon, C. (2020). How to sniff out (and block) BloodHound attacks. Retrieved on 6 December 2020 from <https://www.crowdstrike.com/blog/how-to-block-bloodhound-attacks/>

Marshanski, R., & Kremez, V. (2020). "Front door" into BazarBackdoor: stealthy cybercrime weapon. Retrieved on 15 November 2020 from <https://www.advanced-intel.com/post/front-door-into-bazarbackdoor-stealthy-cybercrime-weapon>

McAfee. (n.d.). McAfee virtual criminology report cybercrime versus cyberlaw - The annual McAfee global study on organized crime and the Internet in collaboration with leading international security experts. Retrieved on 20 June 2020 from <http://www.cs.utsa.edu/~bylander/cs1023/mcafee_vcr_us.pdf>

McAfee. (2020). Take a "NetWalk" on the wild side. Retrieved on 2 November 2020 from <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/take-a-netwalk-on-the-wild-side/>

McCabe, A., Ray, V., & Cortes, J. (2020). Medical organizations with COVID-19 themed phishing campaigns. Retrieved on 6 November 2020 from <https://unit42.paloaltonetworks.com/covid-19-themed-cyber-attacks-target-government-and-medical-organizations/>

McGuire, M., & Dowling, S. (2013). Cyber crime: a review of the evidence. Research Report 75. Retrieved on 31 July 2020 from: <https://www.bl.uk/britishlibrary/~/media/bl/global/social-welfare/pdfs/non-secure/c/y/b/cyber-crime-a-review-of-the-evidence-chapter-1-cyberdependent-crimes.pdf>

Meskauskas, T. (2020). Cerber ransomware removal instructions. Retrieved on 6 December 2020 from <https://www.pcrisk.com/removal-guides/9842-cerber-ransomware>

Microsoft. (2012). Microsoft security bulletin MS12-020 – critical. Retrieved on 6 December 2020 from <https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2012/ms12-020?redirectedfrom=MSDN>

Microsoft. (2018). Now you see me: Exposing fileless malware. Retrieved on 29 November 2020 from <https://www.microsoft.com/security/blog/2018/01/24/now-you-see-me-exposing-fileless-malware/>

Microsoft. (2020). Ransomware groups continue to target healthcare, critical services; here's how to reduce risk. Retrieved on 3 November 2020 from <https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/>

Mitnick, K., & Simon, W. L. (2002). *The art of deception: Controlling the human element of security.* New York, NY: Wiley.

Modus operandi. (n.d.). In *Cambridge Dictionary*. Retrieved from https://dictionary.cambridge.org/dictionary/english/modus-operandi

Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. European Journal of Information Systems, 29(3), pp. 306-321. doi: 10.1080/0960085X.2020.1771222

Nationaal Cyber Security Centrum (2016). Cybersecuritybeeld Nederland 2016. Retrieved on 6 November from <https://www.nctv.nl/binaries/nctv/documenten/publicaties/2016/09/05/cybersecuritybeeld-nederland-2016/CSBN+6-2016+NL.pdf>

Newburn, T., Williamson, T., & Wright, A. (2007). *Handbook of criminal investigation*. New York: Greenberg Publisher.

Newman, L. H. (2020). A ransomware attack has struck a major US hospital chain. Retrieved on 30 October 2020 from <https://www.wired.com/story/universal-health-services-ransomware-attack/>

Nithya, T., Vijaya, K., Subramanian, D., Balamurugan, E., & Shanmugavel, K. (2020). Ransomware deployment and analysis. International Journal of Research and Advanced Development. Retrieved on 3 November 2020 from <http://www.ijrad.com/docs/v4n2/A87.pdf>

NOS. (2020, 19 April). Wuhan komt weer tot leven, maar blijft bang voor een nieuwe uitbraak. [Wuhan comes back to life, but remains afraid of another outbreak]. Retrieved on 15 June 2020 from: <https://nos.nl/artikel/2331009-wuhan-komt-weer-tot-leven-maar-blijft-bang-voor-een-nieuwe-uitbraak.html>

Nurse, J. R. C. (2018). Cybercrime and you: how criminals attack and the human factors that they seek to exploit. *The Oxford Handbook of Cyberpsychology.* doi: 10.1093/oxfordhb/9780198812746.013.35

Paganini, P. (2020). REvil ransomware operators breached healthcare org Valley Health Systems. Retrieved on 6 December 2020 from <https://securityaffairs.co/wordpress/107580/cyber-crime/valley-health-systems-revil-ransomware.html>

Pankov, N. (2020). How coronavirus has impacted work. Retrieved on 29 November from <https://www.kaspersky.com/blog/report-covid-wfh/35244/>

Passeri, P. (2020). Double extortion ransomware attacks and the role of vulnerable internet-facing systems. Retrieved on 13 December 2020 from <https://www.infosecurity-magazine.com/blogs/double-extortion-ransomware/>

Paquet-Clouston, M., Haslhofer, B., & Dupont, B. (2019). Ransomware payments in the Bitcoin ecosystem. *Journal of Cybersecurity, 5(1),* pp. 1-11. doi: 10.1093/cybsec/tyz003

Petters, J. (2020). What is Cerber? Retrieved on 20 November from <https://www.varonis.com/blog/cerber-ransomware/>

Politie. (2020). Cybercriminelen spelen in op coronavirus. [Cybercriminals take advantage of coronavirus]. Retrieved on 13 June 2020 from <https://www.politie.nl/nieuws/2020/maart/31/cybercriminelen-spelen-in-op-coronavirus.html>

Queirós, A., Faria, D., & Almeida, F. (2017). Strenghts and limitations of qualitative and quantitative research methods. *European Journal of Education Studies, 3(9),* pp. 369-386. doi: 10.5281/zenodo.887089

Quintero-Bonilla, S., & Martín el Rey, A. (2020). A new proposal on the advanced persistent threat: a survey. *Applied Sciences, 10(11*), pp. 1-22. doi: 10.3390/app10113874

Ransomware. (n.d.). In *Cambridge Dictionary*. Retrieved from <https://dictionary.cambridge.org/dictionary/english/ransomware>

Richardson, R., & North, M. M. (2017). Ransomware: evolution, mitigation and prevention. International Management Review, 13(1), pp. 10-21.

Rokven, J. J., Weijters, G., Beerthuizen, M. G. C. J., & Van der Laan, A. M. (2018). Juvenile delinquency in the virtual world: Similarities and differences between cyber-enabled, cyber-dependent and offline delinquents in the Netherlands. International Journal of Cyber Criminology, 12(1), pp. 27-46.

Sabarwal, H. (2020). 600% increase in malicious emails amid Covid-19 crisis: UN Official. Retrieved on 2 October 2020 from <https://www.hindustantimes.com/world-news/600-increase-in-malicious-emails-amid-covid-19-crisis-un-official/story-YAcXHHIuDsxQ7l5KaIerEJ.html>

Secureworks. (2019). REvil: The GandCrab Connection. Retrieved on 6 December 2020 from <https://www.secureworks.com/blog/revil-the-gandcrab-connection>

Seebruck, R. (2015). A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model. *Digital Investigation, 14,* pp. 36-45. doi: 10.1016/j.diin.2015.07.002

Smart, W. (2018). Lessons learned review of the WannaCry ransomware cyber attack. Retrieved on 9 October 2020 from <https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf>

Son, D. (2019). LaZagne v2.4.3 releases: Credentials recovery project. Retrieved on 6 December from <https://securityonline.info/lazagne-credentials-recovery/>

Stafford, T. (2020). MOH, OPP assisting in investigation of suspected ransomware attack at Kingston hospital. Retrieved on 6 December 2020 from <https://www.kingstonist.com/news/moh-opp-assisting-in-investigation-of-suspected-ransomware-attack-at-kingston-hospital/>

Subedi, K. P., Budhathoki, D. R., & Dasgupta, D. (2018). Forensic analysis of ransomware families using static and dynamic analysis. *2018 IEEE Security and Privacy Workshops,* pp. 180-185. doi: 10.1109/SPW.2018.00033

Szurdi, J., Chen, Z., Starov, O., McCabe, A., & Duan, R. (2020). Studying how cybercriminals prey on the COVID-19 pandemic. Retrieved on 12 November 2020 from <https://unit42.paloaltonetworks.com/how-cybercriminals-prey-on-the-covid-19-pandemic/>

United Nations Office on Drugs and Crime (UNODC). (February 2013). Comprehensive study on cybercrime. Retrieved on 27 August 2020 from <https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf>

Verma, R., Crane, D., & Gnawali, O. (2018). Phishing during and after disaster: hurricane Harvey. *2018 Resilience Week (RWS),* pp. 88-94. doi: 10.1109/RWEEK.2018.8473509

Victor, K. (2020). Reflective loading runs Netwalker fileless ransomware. Retrieved on 15 November 2020 from <https://www.trendmicro.com/en_us/research/20/e/netwalker-fileless-ransomware-injected-via-reflective-loading.html>

Vissers, T., Spooren, J., Agten, P., Jumpertz, D., Janssen, P., Van Wesemael. M., Piessens, F., Joosen, W., & Desmet, L. (2017). Exploring the Ecosystem of Malicious Domain Registrations in the .eu TLD. *International Symposium on Research in Attacks, Intrusions, and Defenses*, pp. 472-493.

Vizváry, M., & Vykopal, J. (2013). Flow-based detection of RDP brute-force attacks. *Security and Protection of Information 2013,* pp. 131-137.

Wald0. (2016). Introducing BloodHound. Retrieved on 6 December 2020 from <https://wald0.com/?p=68>

Whitney, L. (2020). How to protect your remote desktop environment from brute force attacks. Retrieved on 29 November 2020 from <https://www.techrepublic.com/article/how-to-protect-your-remote-desktop-environment-from-brute-force-attacks/>

Yar, M. (2005). The novelty of 'cybercrime': an assessment in light of routine activity theory. European Journal of Criminology, 2(4), pp. 407-427. doi: 101177/147737080556056

Yin, R. K. (2003). *Case study research: design and methods*. Thousand Oaks, CA: Sage Publications Inc.

Yin, R. K. (2012). *Applications of case study research.* Thousand Oaks, CA: Sage Publications Inc.

Zahra, A., & Shah, M. A. (2017). IoT based ransomware growth rate evaluation and detection using command and control blacklisting. 2017 23rd International Conference on Automation and Computing (ICAC). doi:10.23919/iconac.2017.8082013

Appendix 1

Interview questions

1 Can you briefly elaborate what your experience is with ransomware at hospitals during the pandemic?

2 If possible to assess, what tools were used to gain initial access and/or deploy ransomware at hospitals? (e.g., BazarLoader, TrickBot, Bloodhound, Cobalt Strike, LaZagna)

3 Have you seen offenders using new tools (compared to the situation before the pandemic)?

4 What types of ransomware have you observed since the COVID-19 pandemic, targeting hospitals? (e.g., Maze, Ryuk, Netwalker, EDA2)

5 Did you observe new variants/families since covid-19?

6 When would you label a ransomware variant as 'new'?

7 Did you observe offenders using Ransomware-as-a-Service more often compared to before the pandemic?

8 How did offenders gain initial access to the targets' (hospitals) systems? Could you explain in more detail per method how they have gained access?

9 There were some news articles that attacks against RDP is on the rise. Did you observe such an increase in attacks towards RDP?

10 Did the offenders establish a C2 channel? If so, how did offenders established this? And what did they use it for?

11 Did the offenders use a more stealthy and sophisticated method or fast and simple way?

12 If offenders used a stealthier method, could you elaborate on this? What steps have been taken by the offenders to increase the success of the attack?

13 What did the offenders encrypt? (e.g., files, directories or system?)

14 How did the offenders encrypt the data?

15 How did the offenders extort the hospitals? (e.g., through uploading a ransom note on the desktop wallpaper, through an audio)

16 What did the offenders threatened with if the ransom is not paid?

17 What payment method was used for ransom?

18 Did you encounter a situation wherein the victim paid the ransom? If so, where the files eventually decrypted or not?