C0620 Research Project

A Timeline and Analysis of Ransomware Attacks During the COVID-19 Pandemic

By Sophia Roscoe

Sr694@kent.ac.uk

Supervised By: Jason R.C Nurse

Word Count: 7979

February 27, 2022

Table of Contents

Abstract

Ransomware is a type of malware designed to access, block, and encrypt the victim's personal data until a request is fulfilled. With the estimated average global damage of ransomware increasing from $8 billion in 2018 to $20 billion in 2020 it is not a surprise that there was a significant increase in the number, complexity, and severity of attacks during the COVID-19 pandemic despite the technology only being ~33 years old. The aim of this project was to research all ransomware attacks during the COVID-19 timeline using various news and scientific research outlets to ensure validity and correlate them to a visual timeline of attacks. These statistics are then used to identity trends and patterns in attacks related to significant COVID-19 dates. Being the first pandemic since the invention of the internet, the results of this investigation will provide insight into both human and ransomware behaviour for future pandemics.

This paper aims to display and analysis these attacks from a COVID-19 perspective as well as highlights the vital importance of analysing such a pandemic for future cyber security. I have found that there was a large amount and grouping of attacks in certain sectors such as Government (41), Education (48), Technology (54), and Healthcare (58). This compared to other sectors such as Retail (16) and Services (19) possibly show a focus on these sectors. One reason for this targeting could be to acquire and disrupt valuable Covid-19 research as well as exploit new vulnerabilities created by remote learning. There are also very distinct bunches of attacks in these sectors such September 2020 – December 2020 which seem to coincide with noticeable Covid-19 news and dates. There was a noticeable increase in the use of "double extortion" tactics by ransomware groups such as Ryuk causing a 178% in ransom pay-outs. Finally, one interesting observation is that certain ransomware gangs such as Ragnarok, Avaddon, Darkside, and noticeably Maze emerged and shut down during the Covid-19 timeframe.

Keywords include: Coronavirus, COVID-19, Ransomware, Cyber Security, Cyber-Criminals.

1. Introduction

Ransomware is a form of malware that uses encryption to hold a victim's information/systems at ransom and only allowing them to be encrypted once a request (usually a ransom demand) is fulfilled. Whilst not the most prominent form of cyber-attack, it is the most prominent and destructive form of malware to date despite the technology being comparatively recent as has been on the rise for some time before being expedited during the pandemic. The coronavirus pandemic (COVID-19) is a pandemic that has been a global crisis event since late 2019 and whilst subsided is still ongoing, affecting the social-economic environment. This has resulted in lifestyle changes for 100's of millions of people across numerous countries worldwide. According to recent statistics from the World Health Organisation (WHO) Coronavirus Disease (COVID-19) Dashboard there was 430.3 million confirmed cases and ~5.9 million deaths globally [1] However, it has also had a profound secondary effect on the technology we rely on as cyber-criminals continue to exploit vulnerabilities in the technologies or how they are used.

Since the outbreak and subsequent lockdown there have been numerous reports of breaches in security in student online learning platforms with 50 in the US alone in 2020 [2]. These attacks been made possible due to an increase in reliance in technology but being unable to service remote devices to ensure security standards are maintained. Furthermore, devices used during home learning using untrusted home networks are returned to their school infecting existing systems and allowing for vulnerabilities that can be exploited when the school is most vulnerable during term time or holidays, overall, the resiliency and security of the education information technology system has been severely tested.

Working at home has also become commonplace and raised a new level of cyber security challenges for an already crippled industries and citizens. Ransomware gangs have been able to use both old and new tactics to exploit new vulnerabilities to the point that 64% of people in the US are willing to pay to regain access to their data to reduce the elevated stress, and anxiety they already face [3]. Companies and software vendors themselves also were predominantly blindsided with the demand and security of product further exasperating these problems; something that groups such as Sodinokibi and Maze exploited.

Despite promises from various groups such as Maze and DopplePaymer promising to not attack critical COVID-19 related industries [4] various ransomware attacks have been seen on various healthcare facilities and COVID-19 research

information [5] the value and time criticality of this information makes it an appealing target as well as further solidifies the chance of payment. In response to this increased threat the United Kingdom's National Cyber Security Centre (NCSC) released an advisory on how to mitigate malware and ransomware attacks [6]. This discusses the definition of ransomware along with strategies, actions, and prevention methods to reduce the impact of the infection.

A timeline of cybercrimes has been produced displaying various cyber-attacks in the UK related to COVID-19[7]. However, there is a lack of research in the niche of ransomware and its effect both to and by the pandemic. Also we lack a broader range of attacks related to the pandemic globally partially due to how recent the pandemic is and thus the wider impact remains unclear. With most attacks going unnoticed and being dispersed and sporadically reported by governments, media, incident teams and occasionally scientific journals it is extremely challenging to find a holistic global viewpoint of ransomware attacks and the effects these and the pandemic have on one another. This hinders the ability for governments and organisations to successfully develop appropriate mitigation and protection methods for the current and future environment. This paper should contribute to resolve this.

In this paper I aim to support ongoing research by expanding the search worldwide and present them in a series of visuals in a dashboard showing a simple timeline of events. This and subsequent analysis are useful as it allows us to view 18 months of the pandemic and the attacks that occurred throughout in an understandable and informative format allowing us to identify current trends and tactics used by cyber gangs; providing an insight on how they may react in the future and thus providing us information to respond effectively if such circumstances happen again.

This dashboard includes a scatterplot. This maps various ransomware attacks over the months to show a chronological example of coordinated groups of attacks around the announcement of key global COVID-19 dates, in addition it also maps the attacks to the sectors and countries affected in order to show how the pandemic has influenced the aims of attackers and what is deemed enticing to attack. We expand this scatterplot to focus on specific attacks and their impact both locally and globally. This is complimented with additional information on the different types of cyber gangs to analyse the behaviour of these gangs and to see what their aims may be. To compliment this analysis, we reflect on the broader impact of these attacks for each country how they have affected COVID-19 research, jobs in

their respective sector and how the workforce in these sectors may still be at risk. The chronological nature of the scatterplots well as the clear correlations the other diagrams provide a chronological sequence of attacks and reveal the aims of cyber-criminal gangs during the pandemic. This provides an excellent foundation to build upon with further research whilst standing by itself as a comprehensive piece of literature.

This paper is structured as follows. Section 2 briefly describes the background and functionality of ransomware and why it is used for malicious practises, I then reflect upon notable ransomware attacks in Section 3 and how they have emerged due to past incidents. In Section 4, I discuss the aims and requirements of this project and the methods used along with their limitations. Section 5 will present my results and diagrams with Section 6 focusing on the subsequent analysis combined with small insights on the wider impact on the workforce. Section 7 will conclude my findings and discuss improvements and desires for future work.

2. Background

To guide my understanding and analysis it was vital to understand the basic theory and applications of ransomware as well as wider cybercrime topics. This will also provide a foundation of knowledge to support understanding of this paper as well as allows us to define how complex and impactful ransomware has been during the COVID-19 pandemic. Due to their being various but no universally accepted model related to attacks and cyber-crimes [8, 9, 10], I decided on the UK's Crown Prosecution Service (CPS) categorisation of cybercrime [11]

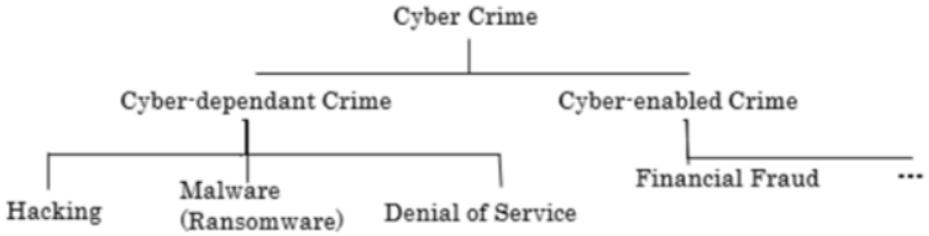

Figure 1 - Cyber-dependent and cyber enabled crimes (focused on cyber dependent crimes) [11]

Ransomware is categorised under cyber-dependant crimes. Cyber-dependant crime is defined as an offence "*that can be committed only through the use of Information and Communications Technology ('ICT') devices, where the devices are both the tool for committing the crime, and the target of the crime*" [11]. Ransomware is defined as "*a form of malicious software that infiltrates a computer or network and limits or restricts access to critical data by encrypting files until a*

ransom is paid." [12]. It attacks a system by being downloaded onto systems via spam mail and RDP (Remote Desktop Protocol) attacks or dropped as a payload by other malware into vulnerable systems. Once executed, ransomware can either lock a computers function or in the case of crypto ransomware such as CryptoLocker [13] encrypts predetermined files (typically SQL, CAD, and tax related files) using an encryption key (e.g. AES [14, 15], RSA [16]) and presents a screen image displaying their demands preventing the user from using their system and access to potentially critical files. This intimidation is why ransomware is known as 'scareware' [17].

Observations have shown that the pandemic has coincided with two evolutions in modern ransomware: Ransomware as a Service (RaaS) and double extortion [17]. RaaS is a form of ransomware developed by a criminal group to be sold to anonymous affiliates with little technical knowledge in return for a share of the profits. The aim of this is to increase the range the ransomware can be used and by the amount of people dramatically increasing the scope of attacks which with new exploitations due to changes caused by the pandemic (remote learning/working etc.) is extremely beneficial to both operators and affiliates. This model has been credited as one of the primary reasons why ransomware attacks have proliferated rapidly both in and outside the pandemic [17]. Examples of this is Ryuk's assumed successor Conti which USA's CISA defines as RaaS [18]

Double extortion is an increasingly used tactic used by groups such as Ryuk, Conti, and Netfilim to coerce victims into paying a random not just by encrypting files but by also threatening to publish sensitive data if the demand are not met, this human operated tactic is most successful on high-profile specific targets and with the increase in sensitive pharmaceutical [19,20] / research[21] information as well as new exploits into sensitive company information through insecure company devices it has been a tactic increasingly used by cyber criminals in recent years[22].

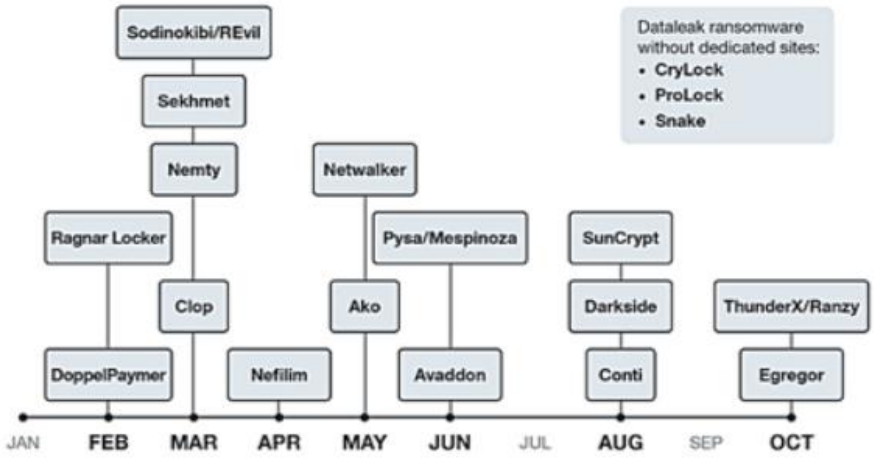

Figure 2 Timeline of notable attacks that involved double extortion in 2020 [17]

3. Literature Review

Even before the pandemic there has been a broad expansion in the role digital technologies have in society. Ranging from shopping, work, and education it is safe to assume the vitality of these systems both for business as well as social interaction. It is not a surprise that cyber-crime has also expanded during this period. Latest reports [23] show that despite malware decreasing by 4%, ransomware has increased by 105% from 2020 to 2021 and a mind-blowing 231.7% from 2019. The regions of the UK and US were hit the hardest with ransomware volumes rising 227% (33.5 million) and 98% (421.5 million) respectively. This increase has also been seen with the cost of ransomware remediation, showing it rising from $0.76 million (USD) to $1.85 million (USD) [24] estimated to reach $20 billion by the end of 2021 [25]. This combined with the new environment caused by the pandemic provides excellent incentive for ransomware gangs to both continue and expand their tactics.

Ransomware and cyber-crime overall requires 3 factors for an attacker to commit a crime successfully: a victim, a motive, and an opportunity. The victim is the target of the attack, the motive is the reason for the criminal to attack and the opportunity is the chance for a crime to be committed. This model has been expanded further in criminology via the idea of Routine Activity Theory (RAT) [26, 27] to describe crimes, others have applied a game-theoretical model of kidnapping to ransomware [28, 29, 30].

These models reflect the fact that attacks have become more sophisticated compared to the early 2000's, as well as much more targeted compared to a "spray and prey" technique. This is dependent on the attacker's motivation whether

financial, revenge or pure enjoyment. During the COVID-19 pandemic ransomware gangs have been quick to take opportunity of specific news and information leaks to attacks industries related to the pandemic. These opportunistic attacks select victims based on how vulnerable they are at one point. With the pandemic increasing the amount of misinformation, time constraints and panic the number of successful ransomware attacks has rose as victims are distracted by other impacts caused by the pandemic, this makes them more susceptible to be deceived by things they would not normally consider, furthermore once deceived they are more likely to make mistakes, panic and comply with the attackers demands then seek outside support due to the time constraints paces upon them along with other human factors, further emboldening attackers.

In addition, industry factors also have an impact with companies now outsourcing a large amount of their technology to allow employees to work from home the security of these devices are reduced severely as they work outside of the company network and technicians no longer have easy access to perform maintenance and upgrades; something the victims may be less educated on. This has provided new avenues for attackers to mislead victims to falling prey to an attack. Other impacts include work pressure, personal changes, mental health conditions, medical issues, or catastrophic events that deeply affect society such fatalities. In the past and present there have been several examples of ransomware gangs using notable events and exploits to maximise their gain, these examples include:

- **Healthcare attacks**: On the 12th May 2017 NHS hospitals were affected by the WannaCry ransomware attack [31]. This attack continued until the evening of the same day when a "kill-switch" was activated preventing further infection. With the partial cause of this being a specific Microsoft Windows vulnerability (none of the 80 NHS organisations affected by WannaCry had applied the advice March 14th 2021 Microsoft office patch to address this vulnerability) the cost of this vulnerability reached £92 million [32] and causes hundreds of surgeries to be cancelled. Recently there have been various healthcare attacks in COVID-19 research facilities such as the eResearch Technology [33] on October 5th that occurred slightly after announcements of 3rd stage clinical trials [34], a surge in COVID-19 deaths [35] and the announcement that US President Donald Trump and the first lady tested positive [36]

- **Infrastructure attacks**: Returning to May 7th 2021, Darkside infiltrated Colonial Pipeline, America's largest fuel pipeline via an exposed VPN password [37, 38]. This resulted not just in ~100GB being extracted and held at a $5 million ransom but a six-day outage causing fuel shortages and hoarding and panic set in. The majority of this ransom was later recovered, and the attackers later apologised and disbanded [39]. Similar attacks occurred on the 27th June in Ukraine when NOTPENYA disrupted power distributors [40]. A monumental number of attacks occurred including JBS foods halting meat processing in Australia [41], and fishing organisations such as NAFO [42]. All of these causing greater confusion, disruption, and panic to an already worried populace.

- **Education attacks**: Education has always been a key target for attackers with University College London being attacked in June 2017 [43] but with the new pandemic forcing online learning as well as increased vaccine research attacks in the education sector has increased significantly. Various K-12 schools have been hit including Toledo Public Schools on September 9th [44] and Baltimore Public Schools [45] halting online learning through infected links and forcing both schools to pay a ransom. Notable lockdowns have also led to an increase in university/ research attacks such as the Netwalker attack on Columbia College Chicago on June 2nd where vital COVID-19 research was held hostage [46].

- **Finance and Technology attacks:** Finance and Technology have always been consistent ransomware targets due to the importance and amount of confidential information and the high reward. Cerber was a particular menace to Microsoft where it was discovered that it had infected more enterprise PC's than any other ransomware family during 2016-2017 [47]. Two significant attacks that occurred during the pandemic was the Travelex attack that occurred 2nd January [48, 49] as information about the pandemic had begun to spread, this disrupted flights, stranding passengers and lead to the company going into administration [50]. The other attack is the Kaseya attack on July 2nd [51, 52]. This multi-chain attack by ReEvil through a fake software update was particularly malicious as over 1500 companies including Acer, and Coop use this software making them all vulnerable forcing mass shutdowns.

In response to these notable attacks multiple guidelines and recommendations have been published by various authorities to protect, prevent, and mitigate these attacks [53, 22]. This is done to both strengthen existing systems as well as provide an education of ransomware and cyber-attacks as a whole. This paper aims to address the gap in ransomware research away from the vague notion of cyber-crime by defining a timeline of attacks to be able to identify key trends to strengthen these industries for any future pandemic and to expand on the impact on citizens and the wider workforce.

4. Requirements and Planning

Whilst there have been numerous attempts in recent months to map and systematically analysis the evolution of cyber-crime during the pandemic [7]: few exist purely for analysing ransomware. There lacks an ability to see a variety of distributed global attacks as seen in this manuscript. This is important as these incidents seriously impact the safety of both local and global economy including human lives, by sorting all attacks into their appropriate sectors and abstracting all unnecessary information into a set of understandable diagrams it provides an ability to see trends otherwise hidden and identify those related to the pandemic.

4.1 Initial Requirements

The aim of this study is to document and analyse COVID-19 attacks globally to complete the purpose of discovering trends between attacks and COVID-19 information with a long term aim of benefiting the wider research community. To do this several requirements need to be fulfilled.

One requirement of the overall paper is to display a clear and reflective of variety of ransomware attacks. This is to ensure that readers are able to understand the analysis being made within the paper and thus understand the connections being made as well as encourage further analysis from the reader. Furthermore by being clear it increases its usefulness to the wider scientific community, providing groundwork for it to be expanded upon in the future. To achieve this, standard cyber-security vocabulary will be used and various visuals are implemented to communicate clear trends in ransomware and the impact of various groups including sector, country, as well as ransomware strains.

In order to present a global, holistic view of ransomware attacks during the COVID-19 pandemic one requirement of the visuals is the ability to map and present a large number of data points. This is necessary to identify trends and

analysis to support specific conclusions in a coherent fashion. It was decided that a scatterplot would be sufficient due to its ability to display hundreds of attacks and provide a timeline of attacks. This is supplemented by stacked bar charts and a choropleth map. These provide a visual representation of global ransomware attacks.

4.2 Approach to Diagram Creation

This section is used to explain the methodology I used to gather information and create my visuals. Within this I will explain the nomenclature and search terms used to efficiently gather necessary COVID-19 information and ransomware attacks, which search materials were used, and the types of sources I chose to use/prioritise. Importantly I also discuss and critique the limitations of my work at various stages.

4.2.1 Nomenclature

There was an extremely large number of ransomware attacks during the COVID-19 pandemic over a wide range of sectors. The pandemic has been referred to with a variety of official names in the English-speaking world including: COVID-19, Covid19, Coronavirus, 2019-nCoV, and SARS-CoV2. Throughout the paper I have used the term COVID-19 to ensure consistency which is reflected by the World Health Organisation [54]. However, I have used all these variations during my search (predominately COVID-19) in order to ensure a wide search base and because the internet and some journals do not the same consistency. Ransomware has the same problem with variations including: ransom-ware, ransom attack, ransomware attack, ransomware virus. All of these have to be considered during research in order to find the highest number of attacks.

Below are the keywords used for searching for ransomware attacks during this phase. This allowed me to widen my reach and attributed to me finding 359+ notable attacks.

Pandemic keywords	COVID-19, Covid19, Coronavirus, SARS-CoV2, and 2019-nCoV
Ransomware keywords	Ransomware, ransom-ware, ransom attack, ransomware attack, ransomware virus, cyber-attack
News outlet keywords	BBC, The Guardian, BleepingComputer, Kaspersky, BlackFog, News, Report,

Sector keywords	Education, K-12, COVID-19 Research, University, Hospital, Medical, Technology, Energy, Industry, Sector

Table 1- Table of key terms used in ransomware attack research

The integrity of research for ransomware attacks was important to ensure that the information collected was correct and supported by viable sources. Because of this certified sources such as BBC as well as sources with a high reputation in cyber security groups such as Kaspersky and BleepingComputer were used to verify attacks.

4.2.2 Construction of the Visuals

The length of the timeline was important to define. As by defining it early, it provided a timeframe to focus my research on and thus allowed me to plan how long this phase would take. It was decided that attacks would be searched for within the 1st January 2020 – 31st August 2021 with the earliest attack being 2nd January 2020[48] and most recent the 26th August 2021[55]. This timeline includes the day the pandemic was officially declared, lockdowns in multiple countries as cases are reported, press releases regarding clinical trials and the release and adoption of the COVID-19 vaccines. The large timeline (18 months) meant that a sufficient number of attacks was reached to fully represent the behaviour of ransomware attacks during this time, allowing higher confidence in the final conclusions. Microsoft Excel was used to store information as the standard for information collection. It also provides various table functions to allow easy filtering and modification of attacks.

Information in the table includes the country that the attack took place, the ransomware strain and group culpable (if known), the sector the victim was located in along with a small description of the attack. Finally, the attack date and date of the article are also recorded. Each attack is attributed to an ID and reference number/URL for the article covering the attack. Due to its size, a subset of this information has been displayed in Table 3 which acts as a baseline for Figure 4.

D3.js[1] was used for construction of the visuals. This open source language works with HTML, CSS, and JavaScript and its purpose is to work with datasets to

[1] https://d3js.org/

create unique data visualizations. This was beneficial for this research as it was necessary to create visualisations that fit my dataset to best represent trends and support my analysis. In addition it is incredibly flexible with a complex syntax. One useful tool was the ability to make all visuals have some form of interactivity; something they all have. For example when one hovers over a ransomware attack on Figure 4 a tooltip will appear containing a description of the attack and its id. This results in a more useful and descriptive visualisation. In this example a zoom function is also available to easily differentiate between bunches of attacks.

Information displayed in the scatterplot includes the date of each attack along with the sector that was impacted. Additionally, the scatterplot also shows the ransomware group responsible for the attack (if known) in order to see the behaviour and target preferences of these groups; otherwise the attack is coloured black. Moreover, the scatterplot also displays a range of dates for notable COVID-19 dates including lockdowns for the UK, US, Spain, Italy, Germany, and France in addition to the three COVID-19 waves in the UK, announcement of phase-3 trials and the date of the initial vaccine rollout. These serve to provide key dates as well as to provide incentives for ransomware gangs to target specific victims. This information continues the entirety of the table.

In addition, there are multiple smaller visuals such as stacked bar charts displaying all attacks per month by country, sector, and ransomware strain respectively as well as a choropleth map displaying the number of attacks per country using a global visual format for better clarification. The structure of the table and visuals is described in further detail in Section 4.3.

This information has been collated using a multitude of sources offering reports of attacks. These sources include established news outlets such as the BBC, Reuters. New sources such as BleepingComputer[2] provided detailed information regarding attacks and their infiltration methods not seen in standard news outlets. Other sources include scientific journals, government and security reports, blogs, and articles. Additionally, various existing lists of ransomware attacks such as Kaspersky[3] and Blackfog[4] were used for comparison to check for missing attacks [56, 57, 58]. Normally blogs and articles would not be considered an academic source due to it being difficult to confirm their credibility however they frequently offer news on ransomware attacks before other sources. In addition, common news

[2] https://www.bleepingcomputer.com/
[3] https://www.kaspersky.co.uk/
[4] https://www.blackfog.com/

outlets frequently choose not to show minor ransomware attacks or present them through a journalistic lens, distorting the facts to grab attention; a blog can show more information for attacks that are less well known. This is important as regardless of the level of publicity these attacks can still pose a tangible threat during COVID-19 and are needed to form a holistic view of ransomware attacks during this timeframe. The scatterplot and other visuals aim to achieve this.

Search engines: Only one search engine was used to create the table and subsequent visuals. This was Google[5]. This US-based engine was chosen due to my familiarity with the engine in addition to it dominating the search engine market. However, additional Google services have been used including Google Scholar[6] to find scientific papers and Google Translate[7] to translate foreign websites into English for easier comprehension.

Time Range: I aimed to create a fully comprehensive timeline associated with the COVID-19 pandemic at that time. As a result, it was decided to start the timeline from January 1st 2020 and the cut-off point not long before the project was started on August 31st 2021. This was to allow adequate time to research an admittedly large timeline as well as to allow time to develop the visuals and analysis findings.

Exclusion Criteria: Despite the extensive list of attacks, specific ransomware attacks were excluded from the results. These included: **a)** attacks and sources behind a paywall or required account creation to obtain **b)** were unable to be confirmed or backed by a source **c)** could not be translated **d)** already existed in other news reports. In addition, attacks sources from engines other than Google were not used.

4.2.3 Types of ransomware attacks

Ransomware, like cyber-crime, is composed of various types. There are various taxonomies for the types of ransomware [59, 60] but they all mostly boil down to 5 main types: Crypto-ransomware, Lockerware, Scareware, Doxxware and RaaS. Al of these exploit victims for a specific purpose. However various attacks are not restricted to one type of ransomware and can encompass multiple types at once. Due to my inexperience with ransomware and time constraints it decided to

[5] www.google.com
[6] https://scholar.google.com/
[7] https://translate.google.co.uk/?sl=de&tl=en&op=websites

restrict ransomware specification to Crypto-ransomware and Lockerware. More information regarding ransomware is seen in Section 2.

4.2.4 Limitations of the table

The purpose of this section is to acknowledge the limitations during research that could have skewed my results and prevented me from furthering the depth of my research and later analysis.

One immediate limitation of the table is the fact that despite my best efforts it is likely that some attacks are not displayed in this table. This is due to some attacks being so obscure that the method searching was unsuccessful and the limitations of a one-person research team has. This can compromise the validity of my final conclusions. Secondly within Table 3 there are two columns called "Article Date" (date the article was published) and "Attack Date" (date the attack occurred).

Regarding "Article Date", I acknowledge that in some cases information in these articles has been updated beyond me acquiring the information. Regarding "Attack Date", despite including the written attack date from each article, it is highly likely that this may not be wholly accurate as an attack may not become obvious until several days after it first infected a system. For clarity Table 3 has been ordered by "Attack Date" to provide a consistent chronological depiction of events.

Furthermore, despite the extensive list of ransomware attacks shown it is not an exhaustive list of attacks. These visuals do not show attacks that were unsuccessful, or ones missed due to time constraints, a lack of reporting or because these attacks did not affect the general public. In addition, it also fails to show further details regarding the various ransomware groups (number of malicious attackers etc.). However, there is enough data to clearly show a correlation between certain COVID-19 events and certain attacks and despite these limitations I have used all available resources to produce a relatively clear image of the ransomware landscape during the COVID-19 pandemic.

4.2.5 Limitations of the visuals

The purpose of this section is to acknowledge the limitations during the creation of my visuals that could have skewed my results and prevented me from making more informative diagrams.

One personal limitation to the quality and clarity of my visuals is my experience in the programming language (D3.js). This being my first time using the language

and the time constraints placed upon me the quality of the diagrams reflects this and could be more professional with more practice.

5. Diagrams and results

The aim of this section is to further examine all ransomware attacks, this will be done through a set of figures and tables which are displayed on a dashboard. Figure 3 shows a snapshot of the dashboard containing all the visuals. The aim of this is to allow easy access to all visuals. This includes Figure 4, 5, 6, and 7 as well as other visuals including a choropleth and tree-map for ransomware attacks per country. It allows access to any of the visuals as well as the project repository in GitHub along with the World Health Organisation COVID-19 dashboard. Whilst highly useful figures 4-7 will be used to represent the visuals during analysis to ensure the highest clarity.

Figure 4 displays a details visual representation of a series of attacks during the COVID-19 pandemic. The scatterplot includes 359 global ransomware attacks during the set timeframe. These are colour-coordinated based on the attacker if known. It also highlights key lockdown dates for countries such as the UK, US, Italy, Spain, France, China as well as the timeframes for the UK's three COVID-19 waves and the vaccine rollout date, it was limited to these countries to avoid an overload of information. These were confirmed as closely as possible with the WHO timeline of events to ensure an accurate representation.

Figure 4 indicates both direct and indirect correlation between announcements and incidents. Direct correlations are when criminals attack directly after or due to an announcement or threat. One possible example is the emergence of CryCryptor ransomware on the 26th June 2020 pretending to be COVID-19 tracing apps on Android [61] after the release of the real app on the 14th March 2020. However, this correlation is not certain. Indirect correlation is when an incident is not directly related to an event. These are prevalent as ransomware was already on the rise before the pandemic and attacks will still continue regardless. However, news events can still influence these decisions inadvertently causing a correlation. For example, discussions of lockdown existed before China's lockdown on the 16th January 2020 however travel company Travelex was attacked on the 2nd January 2020, before it was announced however the motive behind this attack is not concreate and, in both cases, more work needs to be done to confirm the intent behind these attacks.

Table 2 contains the notable global COVID-19 dates shown on Figure 4. These to help find correlations between events and attacks and are uniquely coloured. They contain a "Start Date", "End Date" and a brief description. This table is ordered by "Start Date".

Table 3 categorised a number of global ransomware attacks during the November 2020 period. Due to the size of the table only a snapshot is shown here and like the main table have been ordered by "Attack Date". Within this table the target country and sector have been listed along with a brief description of the attack. It has been logged as to whether the attack aligns most with Crypto-ransomware or Lockerware as explained earlier. Finally, each attack has a unique id for itself to provide easy identification. Both the figure and table abstract detailed explanations of techniques and responses.

Figure 3 - Screenshot of COVID-19 Dashboard

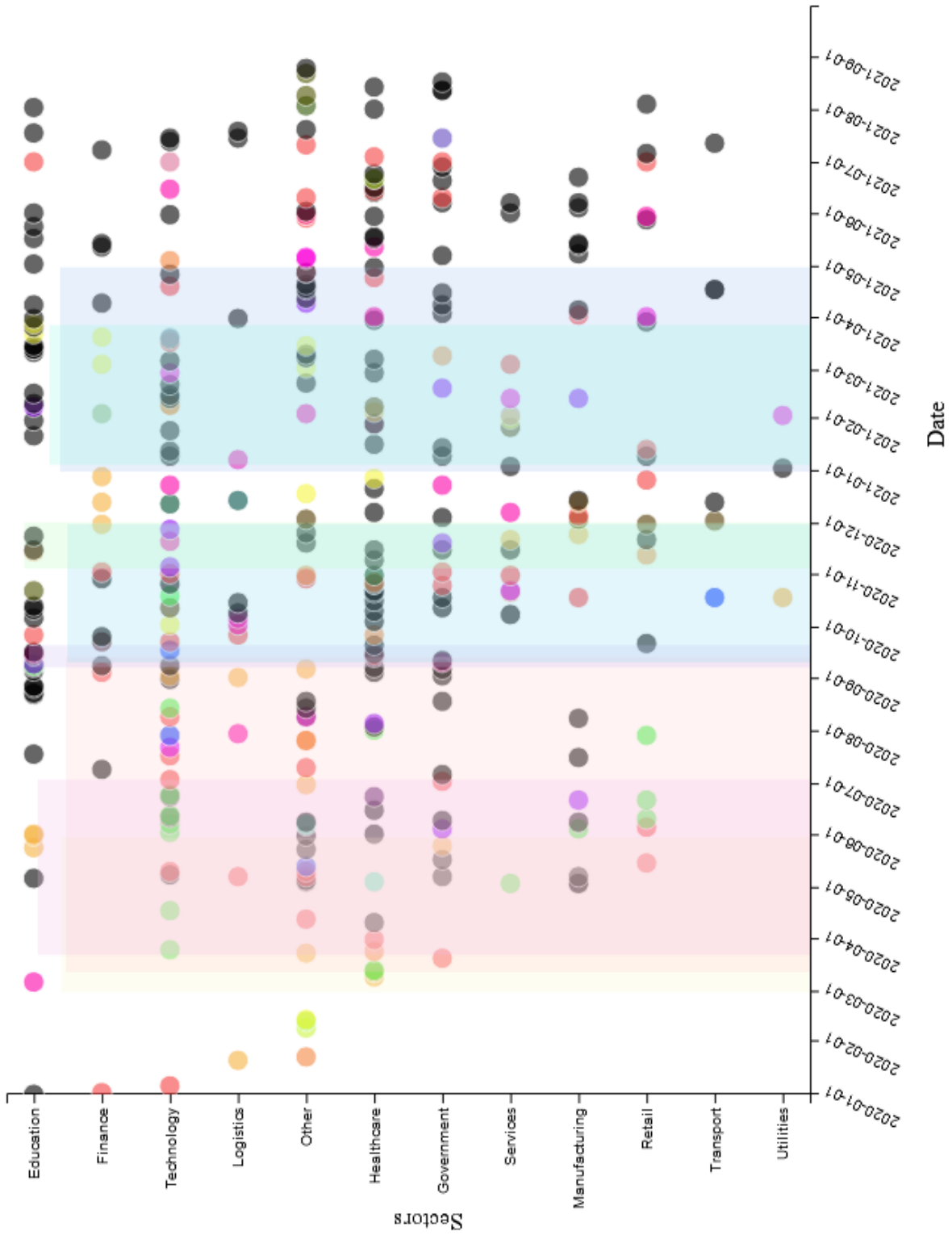

Figure 4 - Scatterplot timeline of ransomware attacks for each Sector during the COVID-19 pandemic

For a version where attacks are not coloured coded by ransomware strain, please see figure A.2 in Appendix A.

	First COVID-19 Wave (UK)
	US Quarantine and Tourist Screening
	UK's 1st Lockdown
	Announcement of phase 3 trials by leading vaccine producers
	Second COVID-19 Wave (UK)
	First vaccine rollout in UK
	Third COVID-19 Wave (UK)
	UK's 2nd Lockdown
	UK's 3rd Lockdown

Table 2 - Colour-coordinated key showing notable COVID-19 dates shown on Figure 4 (shaded rectangles)

Figure 5- Legend for Ransomware Strains in Figure 4

ID	Country	Ransomware Name	Ransomware Type	Sector	Description	Article Date	Attack Date
154	Italy	Ragnar Locker (?)	C	Other	Beverage company Campari Group was suspected to be attacked by the Ragnar Locker gang	2020-11-10	2020-11-01
158	UK	Sodinokibi	C	Services	UK Flagship Group had their IT systems shut down by Sodinokibi after a phishing attack	2020-11-24	2020-11-01
160	Germany	Mount Locker	C	Healthcare	Biomedical and clinical research company Miltenyi Biotec hit by Mount Locker. They are responsible or cell research and have researchers focusing on	2020-11-13	2020-11-01

					COVID-19 vaccines research		

Table 3- Partial table of ransomware attacks during November 2020

To see the full table refer to A.1 in Appendices A.

6. Analysis and Discussion

Research has shown that the acquisition and use of large data sets that includes personal and sensitive information is extremely useful for epidemiological investigations [62]. The scatterplot shown in Figure 4 provides us with a good platform to find trends and analyse the ransomware attacks that have occurred during the pandemic. From the 1st January 2020 and especially during noticeable COVID-19 dates it is clear that ransomware attack frequency increased significantly.

The 359 ransomware attacks presenting in Figure 4 are categorised as followed:

- 59 (16.43%) in Healthcare
- 54 (15.04%) in Technology
- 48 (13.37%) in Education
- 40 (8.71%) in Government
- 23 (6.41%) in Manufacturing
- 19 (5.29%) in Finance
- 19 (5.29%) in Retail
- 16 (4.46%) in Services
- 14 (3.90%) in Logistics
- 6 (1.67%) in Transport
- 3 (0.84%) in Utilities
- 58 (16.16%) in Other

This analysis is useful as it directly allows me to see the most targeted sectors during this timeframe. One immediate insight is the high number of attacks on the healthcare industry. This is expected as it is arguably one of the most important and vulnerable component of a country's critical infrastructure at this time. These attacks have occurred globally including the UK [63], US [64], Czech Republic [65], Canada [66], France [67], and Germany [68] with various gangs including Netwalker, Egregor and Ryuk. These attacks fit the modus operandi of these groups if we assume their aim is to maliciously target specific sectors to capitalise on the current chaos. In this case they believe that health organisations are highly

likely to pay the ransom to both avoid fatalities, and to ensure that valuable COVID-19 research data is not lost or delayed; something vital to prevent further loss of life. In addition, with increased patient numbers and longer working hours causing immense amount of stress employees are increasingly likely to miss signs of a malicious attack (i.e. an email) and less likely to notice an attack occurring thus causing further damage; something ransomware gangs are likely aware of and are keen to exploit. Inconsistent security standards/patches and outdated systems particularly in the UK exacerbate this issue.

This exacerbates the already high pressure on healthcare industry caused by the pandemic as the increase in disposable time combined with the stifling restrictions of lockdown has led to a sharp increase of mental stress and diagnosis as their social and economic circumstances take a toll on people as many coping mechanisms are unavailable. There is a well-documented of negative mental health changes following disasters and previous viral outbreaks [69, 70] and thus it is not unusual that 56% of people a study in the UK were feeling stressed and anxious [71].

Notably multiple ransomware gangs have vowed that they would not target healthcare services during this time including statements from the operators of CLOP, DopplePaymer, Maze and Netfilim [4]. However there have been instances of these gangs accidently or otherwise attacking these services regardless [72]. One considers if this was a tactic to reduce security.

Education has also seen a significant increase in attacks as well resulting in numerous schools closing despite lessons already being interrupted due to the pandemic. These attacks have also spread globally to Germany [73], UK [74], and Netherlands [75] but predominately have been focused on the US with 67% of all education attacks correlated being in the US. Attackers include Netwalker, Clop and ReEvil. Education fits the modus operandi of ransomware gangs due to the large amount of sensitive information; frequently regarding young children. This increase in attacks could be due to the new exploits formed through the introduction of online learning in addition to poorly maintained cyber security. Schools are more likely to pay a ransom to avoid sensitive information being released and to reduce disruption to learning. In addition, universities also saw attacks throughout the pandemic, whilst it's debatable as to whether this is an increase from pre-pandemic it is still important to note the value of research material especially COVID-19 research which ransomware gangs see the value in and aim to disrupt.

Other industries such as Technology and Government have also had a substantial number of attacks. Despite having a larger number of attacks compared to pre-pandemic it is difficult to determine whether this increase is due to the natural increase in ransomware attacks from 2019-2021 or directly because of the pandemic. These sectors have consistently fulfilled the criteria for ransomware groups (sensitive information, ability to pay high ransom etc.). However, it is important to consider the effect the pandemic on the motives and methods of attack. With many companies becoming remote it has led to new vulnerabilities in computer security as company property is connected to unverified networks across the country, technicians unable to perform mandatory security patches and the increased integration and reliance on proprietary software (e.g. Zoom, Slack, Google Meet) as well as non-verbal forms of communication such as email increases the probability of an employee making a mistake or attackers finding an security vulnerability as they trust the security of the company they work for. Overall, COVID-19 inspired ransomware attacks have played upon government backed announcements to exploit the uncertainty and anxiety of society to seek financial profit.

The finance sector has also been affected with 19% of attacks focusing in this sector. This could exacerbate the predicted financial recession. This predicts a spiral for future economic downturn as the combination of layoffs, decreased spending due to lockdown and decreased employment, and the stress this further places on businesses. Some may even turn to cyber-crime themselves to sustain themselves. Contrarily people have also used the pandemic to improve their employment and mental status. Coined the "Great Resignation" 47 million people voluntarily quit their jobs in America alone as workers find themselves with greater bargaining power or wishing to leave to better their own lifestyle with the economic freedom provided by the COVID-19 stimulus package [76]. However, debate as to whether this economic trend was started or merely worsened by the pandemic is ongoing [77].

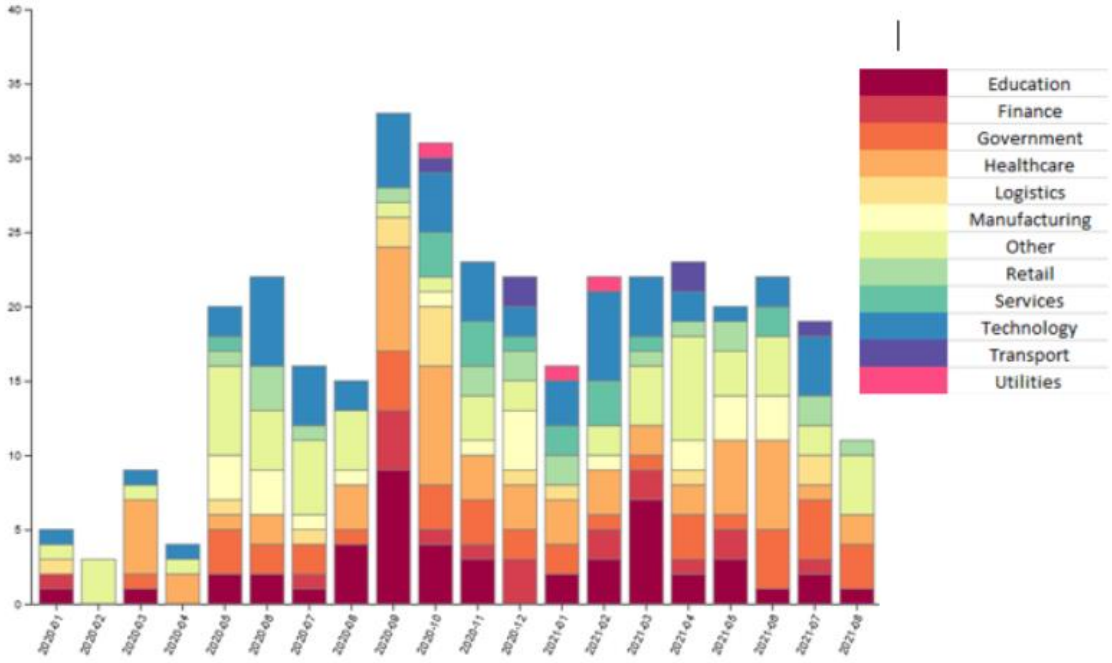

Figure 6 - Ransomware attacks each month (Categorised by Sector)

Figure 5 shows the distribution of attacks per month, this is further categorised by sector. Initial analysis shows an increase in attacks from May 2020, a sharp increase from September 2020 to October 2020 after which there is a slight decrease till the end of the timeline, still above initial levels.

One noticeable trend is the sharp increase of attacks during September-October 2020 period with 33 and 31 attacks respectively totalling up to 18% of all recorded attacks. These numbers seem to correlate with John Hopkins University stating COVID-19 cases had reached 40 million [78, 79], emergence of the Delta variant and announcements of third stage vaccines trials. Figure 4 further supports these findings. This information combined with the strengthening of lockdowns may be the cause as to why the number of attacks on healthcare was the largest during the timeframe at 7 (23% of attacks in September) and 8 (24% of attacks in October) respectively as ransomware gangs use this news to take advantage of the chaos and increased to target the healthcare industry.

Furthermore, it is also important to note the increased number of attacks on education during September 2020 (9 or 29%) and March 2021 (7 or 32%) making it the highest attacked sector in these months. With COVID-19 cases rising during this time schools had switched to online learning and thus required new technologies to function remotely. These recent technologies combined with the extra stress on both teaching and admin staff increases the chance of an attack

occurring unnoticed. This combined with the initial stress and discord of the start of term provides the perfect incentive for ransomware gangs to attack. The same is true for March with the return from half term.

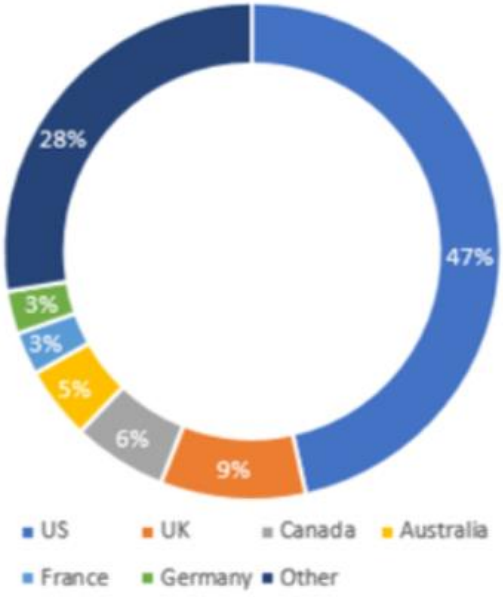

Figure 7 - Percentage of ransomware attacks per country

Figure 6 shows a summary of the main countries that were targets of a ransomware attack and the percentage they constitute for the total number of attacks. As shown the US was the clear frontrunner with 167 total attacks: 47% of the total number of recorded attacks. This is expected due to the US being arguably the largest global superpower with a significant percentage of identifiable global businesses being situated in the country. This notoriety would encourage attacks to occur. The attacks then spread to the UK where 34 attacks (9%) occurred before spreading to various other countries. It is important to mention the large diversity in countries that were attacked. With it counting for 28% of all recorded attacks 45 countries suffered at least one ransomware attack during the COVID-19 pandemic. If we follow the UN's definition of 193 countries [80] 23% of countries have experienced a ransomware attack within this timeframe. It is clear from Table 3 that there is a diverse number of affected countries, and that the US is the most targeted.

All but 4 ransomware recorded contained some form of crypto-ransomware. This makes sense logistically as the primary aim of ransomware gangs is to disrupt exploit their victims for information and money. New instances of ransomware that were discovered in this period such as *DarkSide* (August 2020), *Netfilim*

(February 2020), *Egregor* (September 2020), and *AvosLocker* (June 2021) with the remaining attacks being pre-existing strains such as *ReEvil, Netwalker, Ryuk/Conti, Dharma-Crysis, Mespinoza/Pyza, DopplePaymer.* An example of use is *CXK-NMSL* and *Dharma-Crysis* ransomware being spread through COVID-19 related emails [81].

Despite prolific gangs such as ReEvil and Wizard Spider (Ryuk/Conti) participating in notable attacks, one high profile attack was the Colonial Pipeline attack by DarkSide [37, 38]. DarkSide have explicitly stated they prefer to target high-revenue large organisations in order to extract a large ransom [82] and typically gain access through phishing emails and exploiting remotely accessible accounts. They have also used Remote Desktop Protocol (RDP) to maintain Persistence [82]. In this instance they used an exposed password to a Virtual Private Network (VPN) account and once they had access deployed ransomware to steal sensitive data. Despite receiving a ransom of $2.3 million most was later recovered and DarkSide later stopped all activities due to the backlash [83]; no further attacks were logged by them during this period.

On a larger scale whilst attacks increased in number, ransomware attacks per strain was relatively consistent through the COVID-19 pandemic. It is interesting to see the emergence and termination of the same strains such as DarkSide and Avaddon during this data period however it is unclear whether this is related, directly or indirectly, with the pandemic and would require further research. For many attacks I was unable to find an attacker, or one was not provided (176 or 49% of attacks do not have an attacker associated with it). One reason this may be is that simply the attacker is unknown or not affiliated with any particular gang, with the backlash cyber-attacks can have and the harsh criminal charges if caught, it is beneficial to not reveal your identity. In addition, companies and news outlets may not feel comfortable releasing the attacker's information due to impending investigations or for privacy.

7. Conclusion and Possible Improvements/Future work

The effect and influence the COVID-19 pandemic is like nothing we have ever seen since the invention of the World Wide Web, with the historic and the societal, economical, and even environmental changes being immense and unique; something that ransomware gangs have capitalised upon. Despite including all ransomware attacks, not just those directly related to the pandemic it is clear to

see that there is a loose correlation between COVID-19 events and new announcements and the number of ransomware attack capitalising on the fear to attempt a successful attack.

The findings of this study clearly show that the sectors of Healthcare, Education, Technology and Government were heavily affected by attacks with the months surrounding notable events such as lockdown receiving a slightly higher number of attacks, despite high numbers overall. I discussed the modus-operandi of ransomware gangs and explained how they usually gain access to a system through emails containing malware to plant ransomware, through RDP and compromised accounts with the aim to primarily disrupt and extort people for sensitive information and money (primarily in the form of online currency such as Bitcoin due to its anonymity and ability to use cryptocurrency tumbling services to decrease traceability [84]) with notable examples. RaaS and double extortion have also been briefly explained however future research would be needed to elaborate on the use and effectiveness of these methods. Further analysis on the influence governments and news outlets has been discussed along with an insight on how this pandemic has impacted cyber-security and beyond in the long term.

Despite research into the impact the pandemic has had on cyber-crime having already been performed. I believe this is one of the first times it has been specialised to focus on ransomware with a context of actual global live events. In addition, it is rare to find such as wide timeline for this research due to how recent current events are. However, this study was limited by various factors. For example the current research can be best described as loose and indirectly correlated. It is also difficult to make concrete connections due to the size of the dataset and number of affected countries being too great, as a result some results had to be abstracted in the visuals somewhat decreasing it's accuracy. Additional research should investigate these findings and outline whether a predictive model could prove this relationship. In the future I would like to extend the timeline to April 2022 to include new events in the pandemic such as the Booster Vaccine and the decrease in ReEvil activity. This would provide us with a more holistic view of the pandemic and subsequent ransomware attacks. Making the final analysis much more helpful. I also wish to spend more time on my visuals to make them more comprehensible and constructive. The aim is to collaborate with others performing similar research along with various codified examples of similar research to affirm this conclusion and publish it for the betterment of the scientific community.

8. Acknowledgements

This paper and research has been supported with my exceptional supervisor Jason R.C Nurse. His previous research, knowledge and insight have been integral to my understanding of the subject and I am extremely thankful for his unfailing patience during numerous out-of-hours questions and my final draft. His input was invaluable in producing this paper.

In addition information provided by the World Health Organisation, National Cyber Security Centre and other resources have also been very useful for gathering large scale COVID-19 information and I am thankful of the work they have already performed.

References

[1] W. H. O. (WHO), "Who coronavirus disease (covid-19) dashboard," 2020, thttps://covid19.who.int/, (Accessed 27 February 2022.)

[2] Levin, Douglas A. (2021). "The State of K-12 Cybersecurity: 2020 Year in Review." EdTech Strategies/K-12 Cybersecurity Resource Center and the K12 Security Information Exchange. Available online at: https://k12cybersecure.com/year-in-review/ [Accessed 15 October 2021]

[3] J. R. C. Nurse, "Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit," in The Oxford Handbook of Cyberpsychology. OUP, 2019.

[4] Abrams, L., 2020. *Ransomware Gangs to Stop Attacking Health Orgs During Pandemic*. [online] BleepingComputer. Available at: <https://www.bleepingcomputer.com/news/security/ransomware-gangs-to-stop-attacking-health-orgs-during-pandemic/> [Accessed 28 February 2022].

[5] Ramadan, R., Aboshosha, B., Alshudukhi, J., Alzahrani, A., El-Sayed, A. and Dessouky, M., 2021. Cybersecurity and Countermeasures at the Time of Pandemic. *Journal of Advanced Transportation*, 2021, pp.1-19. [Accessed 21 October 2021]

[6] UK's National Cyber Security Centre (NCSC), Mitigating malware and ransomware attacks, How to defend organisations against malware or ransomware attacks Available online at: Mitigating malware and ransomware attacks - NCSC.GOV.UK (Accessed 27 February 2022)

[7] Lallie, H., Shepherd, L., Nurse, J., Erola, A., Epiphaniou, G., Maple, C. and Bellekens, X., 2021. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, 105, p.102248.

[8] Sabillon, R., Cano, J., Cavaller Reyes, V. & Serra Ruiz, J. (2016). Cybercrime and Cybercriminals: A Comprehensive Study. International Journal of Computer Networks and Communications Security, 4(6), 165-176 [Accessed 10 March 2022]

[9] Brar, H. and Kumar, G., 2018. Cybercrimes: A Proposed Taxonomy and Challenges. *Journal of Computer Networks and Communications*, 2018, pp.1-11. [Accessed 10 March 2022]

[10] Chandra, A. and Snowe, M., 2020. A taxonomy of cybercrime: Theory and design. *International Journal of Accounting Information Systems*, 38, p.100467. [Accessed 10 March 2022]

[11] Cps.gov.uk. 2019. *Cybercrime - prosecution guidance | The Crown Prosecution Service*. [online] Available at: <https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance> [Accessed 10 March 2022].

[12] Varonis.com. 2021. *81 Ransomware Statistics, Data, Trends and Facts for 2021*. [online] Available at: <https://www.varonis.com/blog/ransomware-statistics-2021/> [Accessed 11 March 2022].

[13] D. Gonzalez and T. Hayajneh, "Detection and prevention of crypto-ransomware," *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, 2017, pp. 472-478, doi: 10.1109/UEMCON.2017.8249052. [Accessed 13 December 2021]

[14] CyberNews. 2020. *What is AES Encryption and How Does It Work? | CyberNews*. [online] Available at: <https://cybernews.com/resources/what-is-aes-encryption/> [Accessed 11 March 2022].

[15] O'Kane, P., Sezer, S. and Carlin, D., 2018. Evolution of ransomware. *IET Networks*, 7(5), pp.321-327. <https://doi.org/10.1049/iet-net.2017.0207> [Accessed March 10 2022]

[16] Comparitech. 2021. *What is RSA-4096 ransomware & how to protect against it*. [online] Available at: <https://www.comparitech.com/net-admin/rsa-4096-ransomware/> [Accessed 11 March 2022].

[17] TrendMicro. 2021. *Ransomware-Definition*. [online] Available at: <https://www.trendmicro.com/vinfo/us/security/definition/ransomware> [Accessed 12 March 2022].

[18] Cisa.gov. 2021. *Conti Ransomware | CISA*. [online] Available at: <https://www.cisa.gov/uscert/ncas/alerts/aa21-265a> [Accessed 22 March 2022].

[19] Techcrunch.com. 2020. *TechCrunch is part of the Yahoo family of brands*. [online] Available at: <https://techcrunch.com/2020/04/27/execupharm-clop-ransomware/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cudHJlbmRtaWNyby5jb20v&guce_referrer_sig=AQAAAEM3FtHAtbSlYlBR7f1MmyxzEUIucckadUFbhJBVrYcIpD2SCJs2FlQDAYKFy7XiKadiieIxopKrec0poHUs0OukYyzJ_AVre5Lhu2nAg6kn-kyckn9qJpCFa-6NEvTtubbc4iw0W8TfyW-b7VtFZKbdKs1vjp3Pt6GsBCbtE2_O> [Accessed 12 March 2022].

[20] Consumers, E., 2020. *ExecuPharm Inc Notice of Data Breach to Consumers - Office of the Vermont Attorney General*. [online] Office of the Vermont Attorney General. Available at: <https://ago.vermont.gov/blog/2020/04/17/execupharm-inc-notice-of-data-breach-to-consumers/?=april-17-2020> [Accessed 12 October 2021].

[21] Brusselstimes.com. 2021. *The Brussels Times*. [online] Available at: <https://www.brusselstimes.com/news/belgium-all-news/147433/antwerp-laboratory-becomes-latest-victim-of-cyber-attack> [Accessed 17 December 2021].

[22] Wall, David S., The Transnational Cybercrime Extortion Landscape and the Pandemic: Changes in Ransomware Offender Tactics, Attack Scalability and the Organisation of Offending (August 19, 2021). European Law Enforcement Research Bulletin 2021, Available at SSRN: https://ssrn.com/abstract=3908159

[23] SonicWall. 2022. *2022 SonicWall Cyber Threat Report | Threat Intelligence*. [online] Available at: <https://www.sonicwall.com/2022-cyber-threat-report/?elqCampaignId=13998&sfc=7013h000000MiQZAA0&gclid=CjwKCAiAgbiQBhAHEiwAuQ6BkmbfNdHZWbIdJBPGBn4ut4T3yR5wDxM6JrGQbSMPEUk4O5ClyAmcVxoC7MsQAvD_BwE> [Accessed 13 January 2022].

[24] Sophos. 2021. *The State of Ransomware 2021 Deeper insights than ever into ransoms and encrypted data*. [online] Available at: <https://secure2.sophos.com/en-us/content/state-of-ransomware> [Accessed 5 February 2022].

[25] The National Law Review. 2021. *Ransomware Attacks Predicted to Occur Every 11 Seconds in 2021 with a Cost of $20 Billion*. [online] Available at: <https://www.natlawreview.com/article/ransomware-attacks-predicted-to-occur-every-11-seconds-2021-cost-20-billion> [Accessed 2 November 2021].

[26] Leukfeldt, E. and Yar, M., 2016. Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*, 37(3), pp.263-280. [Accessed 19 November 2021]

[27] Lee, H. and Choi, K., 2021. Interrelationship between Bitcoin, Ransomware, and Terrorist Activities: Criminal Opportunity Assessment via Cyber-Routine Activities Theoretical Framework. *Victims & Offenders*, 16(3), pp.363-384. [Accessed 21 November 2021]

[28] Laszka, A., Farhang, S. and Grossklags, J., 2017. On the Economics of Ransomware. *Lecture Notes in Computer Science*, pp.397-417. <https://doi.org/10.1007/978-3-319-68711-7_21> [Accessed 13 December 2021]

[29] Caporusso N., Chea S., Abukhaled R. (2019) A Game-Theoretical Model of Ransomware. In: Ahram T., Nicholson D. (eds) Advances in Human Factors in Cybersecurity. AHFE 2018. Advances in Intelligent Systems and Computing, vol 782. Springer, Cham. https://doi.org/10.1007/978-3-319-94782-2_7 [Accessed 14 December 2021]

[30] Cartwright, E., Hernandez Castro, J. and Cartwright, A., 2019. To pay or not: game theoretic models of ransomware. *Journal of Cybersecurity*, 5(1). https://doi.org/10.1093/cybsec/tyz009 [Accessed 13 December 2021]

[31] Smart, W., 2018. *Lessons learned review of the WannaCry Ransomware Cyber Attack*. [online] England.nhs.uk. Available at: <https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf> [Accessed 14 March 2022].

[32] nationalhealthexecutive. 2018. *WannaCry cyber-attack cost the NHS £92m after 19,000 appointments were cancelled*. [online] Available at: <https://www.nationalhealthexecutive.com/News/wannacry-cyber-attack-cost-the-nhs-92m-after-19000-appointments-were-cancelled> [Accessed 14 March 2022].

[33] Nytimes.com. 2020. *Clinical Trials Hit by Ransomware Attack on Health Tech Firm (Published 2020)*. [online] Available at: <https://www.nytimes.com/2020/10/03/technology/clinical-trials-ransomware-attack-drugmakers.html> [Accessed 3 October 2021].

[34] Staff, A., 2020. *What We're Reading: J&J Phase 3 Vaccine Trial; Colleges Fueled the Pandemic; FDA's Stricter Vaccine Guidelines*. [online] AJMC. Available at: <https://www.ajmc.com/view/what-we-re-reading-j-and-j-phase-3-vaccine-trial-colleges-fueled-the-pandemic-fda-s-stricter> [Accessed 17 February 2022].

[35] Pérez-Peña, R., 2020. *Coronavirus Deaths Pass One Million Worldwide (Published 2020)*. [online] Nytimes.com. Available at: <https://www.nytimes.com/2020/09/28/world/covid-1-million-deaths.html> [Accessed 16 February 2022].

[36] BBC News. 2020. *Covid: Donald Trump and Melania test positive*. [online] Available at: <https://www.bbc.co.uk/news/world-us-canada-54381848> [Accessed 17 February 2022].

[37] Federal Bureau of Investigation. 2021. *FBI Statement on Network Disruption at Colonial Pipeline | Federal Bureau of Investigation*. [online] Available at: <https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-network-disruption-at-colonial-pipeline> [Accessed 27 December 2021].

[38] Hsgac.senate.gov. 2021. *Hearings | Homeland Security & Governmental Affairs Committee*. [online] Available at: <https://www.hsgac.senate.gov/hearings/threats-to-critical-infrastructure-examining-the-colonial-pipeline-cyber-attack> [Accessed 27 December 2021].

[39] Krebsonsecurity.com. 2021. *DarkSide Ransomware Gang Quits After Servers, Bitcoin Stash Seized – Krebs on Security*. [online] Available at: <https://krebsonsecurity.com/2021/05/darkside-ransomware-gang-quits-after-servers-bitcoin-stash-seized/> [Accessed 31 January 2021].

[40] Tripwire, I., 2017. *Petya Ransomware Outbreak Hits Ukraine, Russia, and Europe*. [online] The State of Security. Available at: <https://www.tripwire.com/state-of-security/latest-security-news/petya-ransomware-outbreak-hits-ukraine-russia-and-europe/> [Accessed 15 March 2022].

[41] Bunge, J., 2021. *WSJ News Exclusive | JBS Paid $11 Million to Resolve Ransomware Attack*. [online] WSJ. Available at: <https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781> [Accessed 14 March 2022].

[42] Seafoodsource.com. 2021. *Northwest Atlantic Fisheries Organization hit by ransomware attack | SeafoodSource*. [online] Available at: <https://www.seafoodsource.com/news/business-finance/northwest-atlantic-fisheries-organization-hit-by-ransomware-attack> [Accessed 26 October 2021].

[43] BBC News. 2027. *Top university under 'ransomware' cyber-attack*. [online] Available at: <https://www.bbc.co.uk/news/education-40288548> [Accessed 28 February 2022].

[44] Ennis, T. and Hegarty, S., 2020. *I-TEAM INVESTIGATION: Major TPS data breach exposes personal information of students, staff*. [online] 13ABC. Available at: <https://www.13abc.com/2020/10/16/i-team-investigation-major-tps-data-breach-exposes-personal-information-of-students-staff/> [Accessed 15 December 2021].

[45] Gordon, J., 2021. *Baltimore Public Schools closed Monday and Tuesday due to ransomware*. [online] Mail Online. Available at: <https://www.dailymail.co.uk/news/article-8997501/Baltimore-County-Public-Schools-closed-Monday-Tuesday-ransomware-attack.html> [Accessed 15 November 2021].

[46] Polidori, K., 2020. *BREAKING: Columbia student information at risk in ransomware attack*. [online] The Columbia Chronicle. Available at: <https://columbiachronicle.com/breaking-columbia-student-information-at-risk-in-ransomware-attack> [Accessed 11 October 2021].]

[47] Microsoft Security Blog. 2017. *Averting ransomware epidemics in corporate networks with Windows Defender ATP - Microsoft Security Blog*. [online] Available at: <https://www.microsoft.com/security/blog/2017/01/30/averting-ransomware-epidemics-in-corporate-networks-with-windows-defender-atp/?source=mmpc> [Accessed 15 March 2022].

[48] Tidy, J., 2021. *Travelex being held to ransom by hackers*. [online] BBC News. Available at: <https://www.bbc.co.uk/news/business-51017852> [Accessed 4 October 2021].

[49] Jay, J., 2021. *Travelex paid $2.3m in ransom to REvil cyber gang*. [online] teiss. Available at: <https://www.teiss.co.uk/travelex-ransom-revil-group/> [Accessed 4 October 2021].

[50] The Guardian. 2020. *Travelex falls into administration, with loss of 1,300 jobs*. [online] Available at: <https://www.theguardian.com/business/2020/aug/06/travelex-falls-into-administration-shedding-1300-jobs> [Accessed 15 March 2022].

[51] Kaseya. 2021. *Kaseya Responds Swiftly to Sophisticated Cyberattack, Mitigating Global Disruption to Customers*. [online] Available at: <https://www.kaseya.com/press-release/kaseya-responds-swiftly-to-sophisticated-cyberattack-mitigating-global-disruption-to-customers/> [Accessed 12 December 2021].

[52] Dailybrief.oxan.com. 2021. *Kaseya ransomware attack underlines supply chain risks*. [online] Available at: <https://dailybrief.oxan.com/Analysis/ES262642/Kaseya-ransomware-attack-underlines-supply-chain-risks> [Accessed 15 March 2022].

[53] Pewtrusts.org. 2021. *Natural Disasters Can Set the Stage for Cyberattacks*. [online] Available at: <https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2021/10/25/natural-disasters-can-set-the-stage-for-cyberattacks> [Accessed 13 March 2022].

[54] World Health Organisation (WHO), "Naming the coronavirus disease (COVID-19) and the virus that causes it," 2020, https://www.who.int/emergencies/diseases/novelcoronavirus-2019/technical-guidance/naming-thecoronavirus-disease-(covid-2019)-and-the-virus-that-causes-it (Accessed 19 March 2022)

[55] IT World Canada - Information Technology news on products, services and issues for CIOs, IT managers and network admins. 2021. *Northern Ontario police force recovering from ransomware attack | IT World Canada News*. [online] Available at: <https://www.itworldcanada.com/article/northern-ontario-police-force-recovering-from-ransomware-attack/457701> [Accessed 31 December 2021].

[56] BlackFog. 2020. *The State of Ransomware in 2020 | BlackFog*. [online] Available at: <https://www.blackfog.com/the-state-of-ransomware-in-2020/> [Accessed 2 November 2021].

[57] BlackFog. 2021. *The State of Ransomware in 2021 | BlackFog*. [online] Available at: <https://www.blackfog.com/the-state-of-ransomware-in-2021/> [Accessed 2 November 2021].

[58] www.kaspersky.com. 2020. *Top Ransomware Attacks*. [online] Available at: <https://www.kaspersky.com/resource-center/threats/top-ransomware-2020> [Accessed 4 November 2021].

[59] Anghel, M. and Racautanu, A., 2019. A note on different types of ransomware attacks. *Cryptology ePrint Archive*. [Accessed 19 March 2022].

[60] crowdstrike.com. 2021. *Most Common Types of Ransomware | CrowdStrike*. [online] Available at: <https://www.crowdstrike.com/cybersecurity-101/ransomware/types-of-ransomware/> [Accessed 13 December 2021].

[61] Osborne, C., 2020. *New ransomware masquerades as COVID-19 contact-tracing app on your Android device | ZDNet*. [online] ZDNet. Available at: <https://www.zdnet.com/article/new-crycryptor-ransomware-masquerades-as-covid-19-contact-tracing-app-on-your-device/> [Accessed 2 February 2022].

[62] W. Price and I. Cohen, "Privacy in the age of medical big data," Nature Medicine, vol. 25, 01 2019.

[63] Ramadan, R., Aboshosha, B., Alshudukhi, J., Alzahrani, A., El-Sayed, A. and Dessouky, M., 2021. Cybersecurity and Countermeasures at the Time of Pandemic. *Journal of Advanced Transportation*, 2021, pp.1-19.

[64] Ahmad Kamal, A., Yi Yen, C., Ping, M. and Zahra, F., 2020. Cybersecurity Issues and Challenges during Covid-19 Pandemic.

[65] Cimpanu, C., 2020. *Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak | ZDNet*. [online] ZDNet. Available at: <https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/> [Accessed 16 October 2021].

[66] Dyrda, L., 2020. *Inside UVM Medical Center's ransomware attack: 11 details*. [online] Beckershospitalreview.com. Available at: <https://www.beckershospitalreview.com/cybersecurity/inside-uvm-medical-center-s-ransomware-attack-11-details.html> [Accessed 21 October 2022].

[67] Archyde. 2021. *Dax hospital disrupted by a "major" computer attack*. [online] Available at: <https://www.archyde.com/dax-hospital-disrupted-by-a-major-computer-attack/> [Accessed 21 October 2021].

[68] RTL. 2020. *Hacker-Angriff verursacht möglicherweise tödlichen IT-Ausfall*. [online] Available at: <https://www.rtl.de/cms/hacker-angriff-auf-uniklinik-duesseldorf-starb-eine-patientin-wegen-einer-erpressung-4615184.html> [Accessed 21 October 2021].

[69] Goldmann, E. and Galea, S., 2014. Mental Health Consequences of Disasters. *Annual Review of Public Health*, 35(1), pp.169-183.

[70] Fancourt, D. and Steptoe, A., 2020. *COVID-19 social study - Nuffield Foundation*. [online] Nuffield Foundation. Available at: <https://www.nuffieldfoundation.org/project/covid-19-social-study> [Accessed 19 March 2022].

[71] The Health Foundation. 2020. *Emerging evidence on COVID-19's impact on mental health and health inequalities*. [online] Available at: <https://www.health.org.uk/news-and-comment/blogs/emerging-evidence-on-covid-19s-impact-on-mental-health-and-health> [Accessed 19 March 2022].

[72] Security Boulevard. 2020. *Maze Ransomware Continues to Hit Healthcare Units amid Coronavirus (COVID-19) Outbreak*. [online] Available at: <https://securityboulevard.com/2020/03/maze-ransomware-continues-to-hit-healthcare-units-amid-coronavirus-covid-19-outbreak/> [Accessed 21 March 2022].

[73] News-rub-de.translate.goog. 2020. *Cyber-Angriff auf die Ruhr-Universität Bochum*. [online] Available at: <https://news-rub-de.translate.goog/presseinformationen/servicemeldungen/2020-05-07-digitale-lehre-laeuft-weiter-cyber-angriff-auf-die-ruhr-universitaet-bochum?_x_tr_sl=auto&_x_tr_tl=en&_x_tr_hl=en-GB&_x_tr_pto=nui> [Accessed 4 November 2021].

[74] Peterboroughtoday.co.uk. 2021. *Peterborough schools and college hit by ransomware attack*. [online] Available at: <https://www.peterboroughtoday.co.uk/news/crime/peterborough-schools-and-college-hit-by-ransomware-attack-3172293> [Accessed 6 November 2021].

[75] The Scientist Magazine®. 2021. *Hackers Bring Dutch Research Funding Agency to Standstill*. [online] Available at: <https://www.the-scientist.com/news-opinion/hackers-bring-dutch-research-funding-agency-to-standstill-68521> [Accessed 12 November 2021].

[76] Curtis, L., 2021. *Why The Big Quit Is Happening And Why Every Boss Should Embrace It*. [online] Forbes. Available at: <https://www.forbes.com/sites/lisacurtis/2021/06/30/why-the-big-quit-is-happening-and-why-every-boss-should-embrace-it/> [Accessed 23 March 2022].

[77] Harvard Business Review. 2022. *The Great Resignation Didn't Start with the Pandemic*. [online] Available at: <https://hbr.org/2022/03/the-great-resignation-didnt-start-with-the-pandemic> [Accessed 23 March 2022].

[78] Npr.org. 2020. *40 Million Coronavirus Cases Are Now Reported Worldwide*. [online] Available at: <https://www.npr.org/sections/coronavirus-live-updates/2020/10/19/925325563/40-million-coronavirus-cases-are-now-reported-worldwide?t=1647897491425> [Accessed 21 March 2022].

[79] Gisanddata.maps.arcgis.com. 2019. *ArcGIS Dashboards*. [online] Available at: <https://gisanddata.maps.arcgis.com/apps/dashboards/bda7594740fd40299423467b48e9ecf6> [Accessed 21 March 2022].

[80] Nations, U., 2022. *About Us | United Nations*. [online] United Nations. Available at: <https://www.un.org/en/about-us> [Accessed 22 March 2022].

[81] Www-freebuf-com.translate.goog. 2020. ***疫情防控期的几****类网络安全威胁分析与防范建议 - FreeBuf****网络安全行业门户***. [online] Available at: <https://www-freebuf-com.translate.goog/company-information/227585.html?_x_tr_sl=zh-CN&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=nui,sc> [Accessed 16 October 2021].

[82] Varonis.com. 2021. *Return of the Darkside: Analysis of a Large-Scale Data Theft Campaign*. [online] Available at: <https://www.varonis.com/blog/darkside-ransomware> [Accessed 22 March 2022].

[83] Nytimes.com. 2021. *DarkSide, Blamed for Gas Pipeline Attack, Says It Is Shutting Down*. [online] Available at: <https://www.nytimes.com/2021/05/14/business/darkside-pipeline-hack.html> [Accessed 22 March 2022].

[84] Financialexecutives.org. 2021. *The Wild World of Crypto Ransomware Payments*. [online] Available at: <https://www.financialexecutives.org/FEI-Daily/October-2021/The-Wild-World-of-Crypto-Ransomware-Payments.aspx> [Accessed 23 March 2022].

Appendices A

A.1 Continuation of table of ransomware attacks during November 2020

ID	Country	Ransomware Name	Ransomware Type	Sector	Description	Article Date	Attack Date
153	Japan	Ragnar Locker	C	Technology	Capcom hit by Ragnar Locker attack claiming to have 1TB of stolen data from various offices worldwide.	2020-11-05	2020-11-02
155	Brazil	RansomExx (?)	C	Government	Gigantic attack by RansomEXX on the Brazilian Superior Court of Justice (STJ)	2020-11-06	2020-11-03
165	Australia	ReEvil	C	Finance	Nexia Australia and New Zealand were hit by ReEvil ransomware. 76GB of data was claimed to be stolen but Nexia denies this	2020-11-16	2020-11-03
157	Taiwan	DopplePaymer	C	Technology	Taiwanese electronics giant Compal was hit by DopplePaymer ransomware. This attack is said to have hit 50% of their computer fleet.	2020-11-09	2020-11-06
159	US	?	C	Healthcare	Medical billing company Timberline Billing Service LLC hit by unknown ransomware attack. The company has vowed to improve their cyber security	2020-11-11	2020-11-10
162	Chile	Egergor	C	Retail	Retail company Cencosud was hit by an Egregor Ransomware attack affecting multiple stores.	2020-11-14	2020-11-13
176	US	Ryuk	C	Education	Mutliple K-12 schools were hit by Ryuk ransomware by manage to avoid a data leak	2020-12-02	2020-11-15
161	US	?	C	Healthcare	Americold was hit by an unknown attack in November. This is important as they are responsible for	2020-11-16	2020-11-16

					cold storage for COVID-19 vaccines.		
164	US	?	C	Services	Lehigh Valley Library in Pennsylvania had its servers forced offline from an unknown attack. However they were later restored.	2020-11-17	2020-11-16
166	US	?	C	Government	Jackson County in Oregon was hit by an unknown ransomware attack from a website they were hosting (Managed.com).	2020-11-19	2020-11-16
174	US	?	C	Education	Baltimore Public Schools was hit by an unknown attack affecting 115,000 students.	2020-11-29	2020-11-16
168	UK	?	C	Other	Manchester United Football Club were hit by an attack later revealed to be ransomware. Whilst initially worried the club stated that due to protocols they were prepared.	2020-11-26	2020-11-20
173	US	DopplePaymer	C	Government	Delaware County in Pennsylvania were hit by the DoppelPaymer gang forcing systems to be taken offline.	2020-11-29	2020-11-20
172	US	Conti	C	Technology	Advantech were attacked by Conti who demanded a $14 million ransom to avoid a double extortion tactic.	2020-11-30	2020-11-21
167	South Korea	?	C	Retail	South Korean fashion and Retail company E-Land had to close nearly half of their stores after an unknown ransomware attack.	2020-11-22	2020-11-22
169	Australia	Netwalker	C	Services	Law In Order, an Australian supplier of Services to law firms were hit by the Netwalker gang.	2020-12-03	2020-11-22
170	Denmark	?	C	Education	Ritzau, a large indepandant news agency had to shut	2020-11-25	2020-11-24

					down their systems after an unknown ransomware attack. Data was taken but they refuse to pay the ransom		
179	Brazil	RansomExx	C	Manufacturing	Aerospace corporation Embraer stated that they had been hit by the RansomEXX gang, they refused to negotiate and later their data was published online.	2020-12-07	2020-11-25
175	Netherlands	?	C	Other	Endemol Shine, disclosed that they had been hit by the DopplePaymer gang resulting in personal and commercially sensitive data being compromised.	2020-11-29	2020-11-26
183	Mexico	DopplePaymer	C	Technology	Electronics giant Foxconn were hit by DopplePaymer ransomware at a facility during the Thanksgiving holidays. Some fles were later published.	2020-12-07	2020-11-28

A.2 Scatterplot showing all ransomware attacks during COVID-19 timeline (non-colour coded version)