Minimization of Cyber Security Threats Caused by COVID-19 Pandemic

Dr Liqaa F. Nawaf, Dr Chaminda Hewage, Dr Fiona Carroll

Cardiff School of Technologies, Cardiff Metropolitan University, UK

{LLLNawaf, CHewage, FCarroll}@Cardiffmet.ac.uk

Abstract. While the world is preoccupied in its struggle with the Coronavirus pandemic, cyber-criminals are busy every day, spreading their own viruses, by phishing emails, data breaches, frauds, denials of service, and taking advantage of the vulnerabilities created by this crisis. In many ways, we, as a nation, are handing over our data without realizing it, without fully thinking it through or even being aware of cyber threats, which will ultimately have a tremendous impact on governments and citizens both personally and at work. The goal of this paper is to investigate the correlation between the cyber-attacks before the coronavirus and during the coronavirus in order to build an understanding of what is happening. To optimize cyber security and provide effective ways to tackle cyber security attacks during COVID-19 or something similar, we need to consider extra precautions and take a more secure approach to protection. To minimize the universal risks of data breaches and other cyber incidents, we need to enforce practical steps to deal with and if possible limit those risks. This requires not only thoughtful consideration but also a good understanding of the opportunities that COVID-19 provides to cybercriminals. The aim of this research paper is to investigate the growth of and reasons for the increase of cyber-attacks during the COVID-19 pandemic. In order to make better cyber security decisions, we need to address and maximize the level of cyber security awareness and precaution taken during COVID-19. A set of practical steps to minimize the risk of cyber-attack is provided to compensate for the vulnerabilities associated with COVID-19.

Keywords: Cyber-attack, COVID-19 Pandemic, Cyber-criminal, Risk, Phasing, Data Breach.

1 Introduction

All over the world millions of network engineers, technicians, and system administrators are working determinedly to maintain safe and effective cyber systems for everyone. In a scenario where millions more people are working from home, they are faced with a high volume of people online, high network demands and consequently a rising number of cyber threats. The COVID-19 pandemic is a world-wide threat to health and society that requires effective and immediate action by governments, businesses and individuals. From the data collected, we can see that a number of threats have come from people using COVID-19 related lures to deploy malware.

Clearly, we feel that certain businesses have a significant role to play in reducing the possibility of cyber threats on society. It is also believed that prompt and effective action will reduce the risks to employees and the long-term costs to businesses. For example, the restrictions on face to face communication and social distancing requirements have made it vital for many households and organizations to go online to connect with work colleagues and family. This opens up opportunities to cyber-criminals and hackers to exploit new weak points in the access to data and networks; the sheer volume of people socialising and working online gives these people more ways to install a malicious code or software on poorly protected computers.

Many organizations have implemented an information security management system to protect their data and networks, but it is the human element that poses the greatest threat. All organizations, which depend on business continuity, have found that the COVID-19 pandemic has created such a high risk for their day-to-day activities that they have had to reassess their security strategies carefully. For example, phishing emails went from 25,000 a day to 125,000 – that equates to 500 per cent increase [1]. This indicates that the risk exists and is serious, whereas the firewalls included within the local broadband routers are adequate for certain attacks but not perhaps for the criminal attacks that are on the rise in response to the increased personal use of computers and the unprecedented amount of homeworking. Moreover, while the NHS is working hard to mitigate the health risks from Covid-19, the cyber criminals are in full control of malicious code which they install to increase the risks of a cyber-attack. This paper will investigate a sensible and practical set of steps to limit those risks and help secure transactions online in these very difficult times. The paper is organized as follows: Section 2 provides a literature review of related approaches. Section 3 describing and applying a layered approach to cyber security: From multi-factor authentication to cyber security awareness. Followed by section 4, A COVID-19 ‘Data’ perspective on cyber security that discuss cyber threats. Having evaluated the results, we then proceed the final section to draws some conclusions.

2 Related Work

Cyber attackers, including those from aggressive nation-states, are more and more focused on targeting their actions on critical infrastructures [2]. Cyber criminals come in many different forms, each has an individual purpose, such as theft or interrupting communication and cause a significant loss of time and money. For example, the International Criminal Police Organization has recently exposed a €1.5m face-masks scam in Germany, Ireland and the Netherlands [3]. Preying on the world's desperate need of face masks at present, some money was swiftly wired to Nigeria, but luckily the fraud was prevented by action from Interpol. In fact, successful attacks are not always sophisticated; even an unskilled attacker can sometimes achieve his/her illegal aims.

The issue, as realized in many of the recent news accounts of data breaches, is that too few people know enough about these cyber security threats to protect private and powerful information [4]. Therefore, it is crucial for users to understand the cyber security issues that might affect them and to be equipped to combat cyber-attacks. To be specific, a recent survey stated that Denial of Service (DoS) attacks are considered to be the most widespread. They interrupt online services for one and sometimes many end-users [5]. Clearly, knowing about these types of attack may reduce the danger to their privacy and security.

As recent news reports highlight, the vulnerabilities and threats generated by the COVID-19 pandemic have demonstrated the high risk to cyber security. Cloudflare [6] which is the foundation supporting infrastructure, applications and teams, states that over the past few weeks online threats have risen to almost six times their usual level. The current pandemic provides a new impetus for cyber-attacks. One UK news report [7] claims that hacking and phishing attempts have risen by 37% month-on-month throughout the pandemic, whereas on some days, security was obstructed between four and six times as often as usual. Research from DARK Reading [8] also indicates the increase in threats and highlights. the top threat as that of phishing (55% of respondents), followed by wrong and fake information about COVID-19 on websites, malware, and ransomware attacks. The BBC News [9] stated that social networks such as Twitter, YouTube, TikTok and Facebook have nurtured COVID-19 misinformation, "fake news", including viral messages asserting that 5G is related to Covid-19. YouTube has since banned these videos and other incorrect/fake statements.

It is clear that whilst risk has risen and the effects of threat are continuous, people worry that there will be a long-term effect on society and the cyber security industry. Thus we believe that further awareness and precautions are essential, we need more sophisticated approaches (set of steps/ procedures) to equip people with the knowledge to avoid a malicious attack.

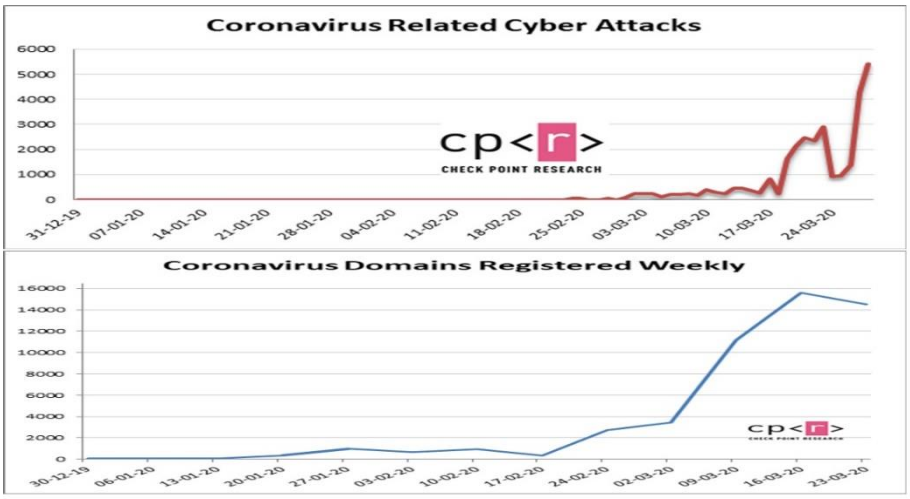

Fig. 1. Coronavirus-related cyber-attacks and domains registered. [10].

The graph shown in **Error! Reference source not found.** demonstrates all the coronavirus-related cyber-attacks that have been identified by Check Point [10]. As can be seen, different types of threat technology extend across networks, endpoints and mobile devices. The graph highlights a continuous and rapid increase in cyber-attacks. However, it is not astonishing that the pandemic has caused a sharp increase. In recent weeks, a significant growth in the number of phishing attacks has been perceived by websites posing as Netflix sites [11]. This indicates the correlation between cyber-attacks and the increase in vulnerabilities caused by the pandemic.

Dark web-based drug (medical) dealing is on the rise. COVID19 has caused a scarcity of essential medical supplies (e.g. Paracetamol, PPE, hand sanitizers) due to problems of sourcing and supply. Cyber criminals have used this opportunity to advertise these goods on the dark web at significantly reduced prices to the large population of users who have tended for some time to buy certain items from this source. The items on the dark web market range from N95 masks, hand sanitizers, COVID-19 related drugs such as Chloroquine and even sell home testing kits for COVID-19 from some vendors. Since most of these products are new to the dark web marketplace, they carry no reviews from buyers. Hence, buyers inherently risk not getting what they have paid for. It seems that the dark web is also facing supply chain problems due to the pandemic [12]. Hence the amount of Bitcoins spent on the dark web has over the last two months has gone down. Fig. 2 shows, according to the blockchain analysis company, Chainalysis, that the value of Bitcoins sent from Chinese exchanges to dark net markets has fallen significantly.

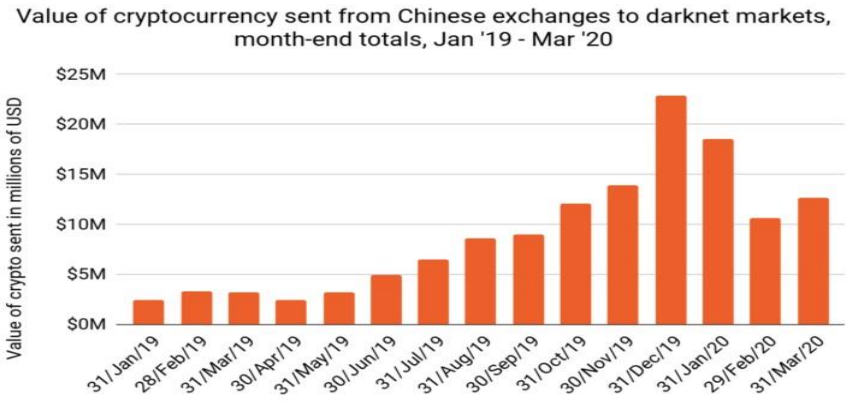

Fig. 2. The value of Bitcoin sent from Chinese exchanges to dark net markets [12].

3 Applying a Layered Approach to Cyber Security: From Multi-Factor Authentication to Cyber Security Awareness

The previous section has indicated from the cyber security perspective the great increase of cyber-attacks and the impact of COVID-19 in the form of cyber criminals exploiting the crisis. These cyber-attacks need to be known by the general public to prevent these and other cybercrimes from growing.

Currently, the healthcare specialists and hundreds of thousands of allied professionals are using the full capacity of their knowledge and resources to fight the current pandemic, though no one can as yet predict which approach will achieve the most successful cure. As regards viruses of the other type, we feel that everyone can play a part by finding and sharing cyber security knowledge to create a solution that can minimize cyber-attacks. Some companies are working to identify measures used in banking and other services where sensitive data is held to better defend systems from cyber-attack. The technique is commonly known as two-factor or multifactor authentication, which uses an application installed on a smartphone, or sends out an SMS or email to verify who is logging in. This technique is essential for protecting data from a cyber-attack and depends on more than simply relying on knowing the username and password to access a secure system. To reduce the current risk level, a whole series of procedures need to be accepted and end-users need to be aware of the threats to their security and safety. Moreover, in light of COVID-19, the joint advisory staff from the UK's National Cyber Security Centre and the USA's Cybersecurity and Infrastructure Security Agency are working with law enforcement and industry partners to find new ways to detect and prevent malicious COVID-19 cyber activities [13]. We feel that to improve the resilience against the phishing attack and/ or other criminal attacks we should extend the defenses to combine the more technical measures with a heightened cyber security awareness.

4 A Covid-19 'Data' Perspective on Cybersecurity

Having demonstrated the possibility of minimizing the risk level, we now report further work that was done to expand the range of measures and investigation of cyber-attack. A simple algorithm was used to generate an appropriate data set taken from MISP Project-Threat Sharing, which is an open source software program and set of standards to share, create and confirm threats to intel and intelligence. The data set listed places at random that are exploiting the impact of the COVID-19 pandemic. The data set of the intrusion detection systems for a given attribute was generated. This data set contains various categories, types, values, object names and countries/regions. We analyzed the data set as follows to evaluate the solutions in this paper:
The data set included different types of cyber threat during the current pandemic which have to be minimized or if possible stopped.
The data set contains various types of attachment for different categories of malware attack, (see Fig. 3A and 3B) showing that the most often used attachment to deploy malware on the victim's computer is a file. Different categories of malware attack reveal that a great number of phishing and malicious attacks were used against victims. In addition, a small number of payload, Trojan, ransomware, adware, agent tesla, and spam, was applied. This indicates that phishing awareness must be a highly eligible way to help victims mitigate the cyber threat.

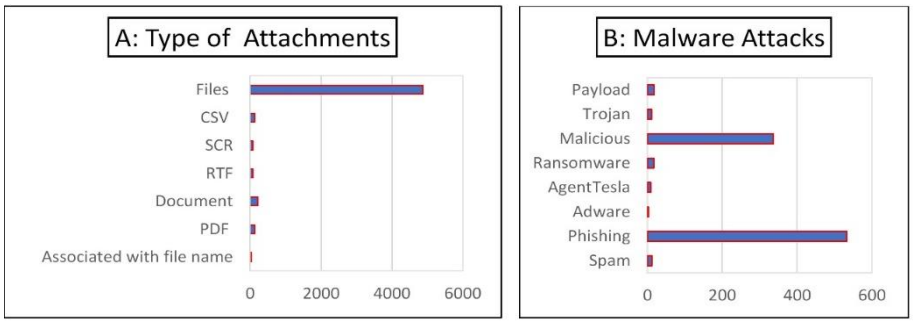

Fig. 3. (A) Type of attachments and (B) value of malware attacks

According to the indicators of compromise (IOCs), it is evident that there is an increased cyber activity related to COVID-19. Cyber criminals use the panic situation or the uncertainty created by the pandemic to lure general users to click on a malicious link or use some other path to hack into a victim's computer and steal data or to direct further attacks. This has been facilitated by the nation-wide lockdowns currently imposed in many countries. As a result, many more people are using the Internet to learn, socialize and work from home. This has paved the way for the would-be attackers to invade users' privacy and security controls. According to Fig. 4, it is clear that these have increased their domain name registration with some form of reference to COVID-19. These domain names can be used by cyber criminals for disinformation, malvertis-

ing and as malicious domains which closely align with genuine websites (Cyber-squatting). Hence, domain names need to be closely monitored for their use in order to tackle all forms of malicious activity not only during the present pandemic but also afterwards. A significant increase of hostnames which refer to COVID-19 are also apparent. These staged usernames can be used to lure victims in phishing campaigns. Furthermore, a number of malware payloads have been discovered. Some of them are being currently investigated by organizations such as Virustotal. It is highly likely that these malwares were not generated during this pandemic, but have lately been reshaped for activation during the pandemic.

The way that cyber criminals work may not have changed since before COVID-19. They have simply seen an added opportunity thanks to the infodemic and increased use of the Internet. While the main attack weapons used by the criminals remain the same (e.g. phishing attacks), they may change in format and appearance to attack via the disease. The key solution is user awareness. While more than a quarter of the global population is in lockdown, the hackers roam freely. They will use every opportunity available for them to steal important data or harm individuals or organizations. Hence it is important to increase the awareness of the public and ask them to always use standard security measures for and preserving privacy.

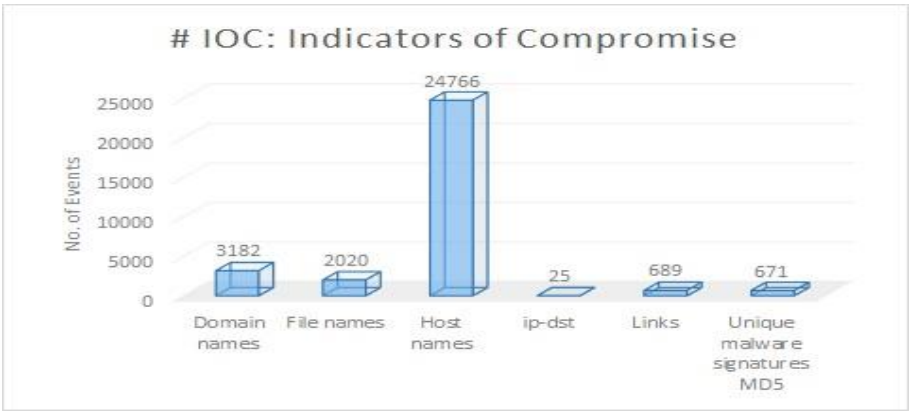

Fig. 4. IOC for Cyber related incidents with COVID-19.

Endsley talks about the importance of situational awareness for humans to make decisions within a wide range of environments [14]. She defines situational awareness as the perception of the elements in the environment, comprehension of the situation, and projection of future status. Aligning with this ideology, we envision a set COVID-19 cyber security awareness guidelines as, first, supporting the user in becoming aware of the elements in their online environment. As we have found in this research, 'hostnames' linked to COVID-19 are proving to be frequent sources of threat, and as end-users we need to be cautious of these COVID-19-related sites. Second, on these websites (see Fig. 5, which highlights daily reports and city reports of COVID-19 as types of websites carrying threats), and/or receiving emails about COVID-19-related subjects, we need to know how to identify malicious characteristics and elements such as

files, or inferences drawn from these files or, in sum, phishing attacks. Third, particularly during the present crisis, we need to have the foresight to predict from these inferences so as to protect everyone's security. Although the COVID-19 is affecting over 210 countries and people across the world are facing the same devastating impact from its spread, they should be aware that cyber criminals feel no sympathy and that they will take advantage of people's fear to attract them and lure them to the trap. Therefore, we feel that this three-pronged approach (supported by reliable data) will help support end-users to identify the visible threats, reduce their areas of weakness and enhance their cyber security awareness, especially these days.

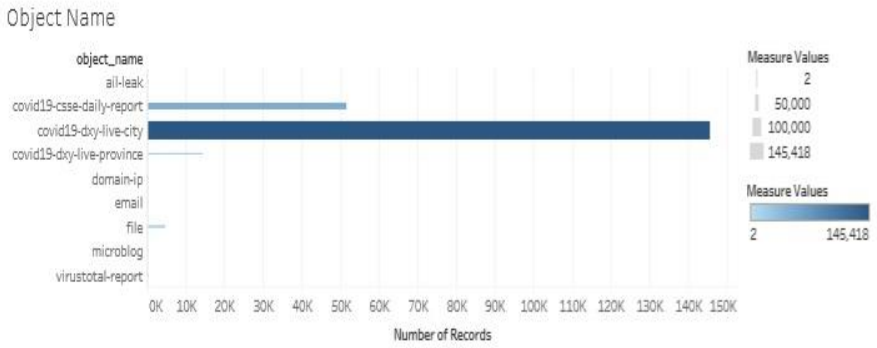

Fig. 5. The main source of cyber threat and number of records/ websites carrying threats.

5 Conclusion

The vulnerabilities and threats associated with COVID-19 pandemic have been highlighted and discussed in the previous sections. To mitigate those risks, security protection such as providing an employer's internal computer system with the following is needed: imposing a working time restriction even on staff who work from home; and employing the Multifactor Authentication of the state of the pandemic. We advocate for a layered approach to cyber security and the practical steps to minimize and limit those risks must be taken. In addition to the technical, people must be made aware of the threats in order to enable them to avoid COVID-19 fake news and deception completely. The social networks claim to take significant steps in fighting awkward coronavirus posts and suggesting or calling for apps to catch fake COVID-19 news that could cause harm [9]. As we have seen from the data, the threats are extensive and it is very challenging to eliminate all the risks of a data breach and other cyber-attacks in the face of the fast changing and increasing uncertainty of coronavirus in the population. Saying that, we feel that a layered approach that will provide end-users with the required knowledge to be able to identify malicious characteristics and other adverse cyber signals is essential. Furthermore, the government and organizations must be capable of reacting quickly because of the possibility of non-stop cyber-attacks if action is not taken.

References

1. N. Tyler, “Covid-19 cyber security threat to impact businesses,” newelectronics, 1 April 2020. [Online]. Available: https://www.newelectronics.co.uk/electronics-blogs/covid-19-cyber-security-threat-to-impact-businesses/225701
2. R. Thatte, “Is cyber security the biggest technological challenge that we are facing today?” 6 July 2018. [Online]. Available: https://scet.berkeley.edu/reports/is-cyber-security-the-biggest-technological-challenge-that-we-are-facing-today/. [Accessed 4 April 2020].
3. Admin, “Interpol foils €1.5m face masks fraud traced to Nigeria,” 16 April 2020. [Online]. Available: https://observerstimes.com/2020/04/16/interpol-foils-e1-5m-face-masks-fraud-traced-to-nigeria/. [Accessed 16 April 2020].
4. G. L. Weiss, “Network Effects Are Becoming Even More Important On Emerging Platforms,” 18 March 2018. [Online]. Available: https://www.forbes.com/sites/startupnation-central/2018/03/18/why-a-network-effect-is-the-only-way-your-startup-can-win/#1ef866de7527. [Accessed 4 April 2020].
5. C. Kolias, G. Kambourakis, A. Stavrou and S. Gritzalis, “Intrusion Detection in 802.11 Networks: Empirical Evaluation of Threats and a Public Dataset,” *IEEE Communications Surveys & Tutorials,* vol. 18, no. 1, pp. 184 - 208, 2016.
6. CloudFlare, “Cloudflare was built for this.,” 28 March 2020. [Online]. Available: https://www.cloudflare.com/en-gb/. [Accessed 5 April 2020].
7. P. Muncaster, “Cyber-Attacks Up 37% Over Past Month as #COVID19 Bites,” UK/ EMEA News Report, 1 April 2020. [Online]. Available:https://www.infosecurity-magazine.com/news/cyberattacks-up-37-over-past-month/#at_pco=smlrebh-1.0&at_si=5e89dbda83e6cab5&at_ab=per-2&at_pos=3&at_tot=4. [Accessed 4 April 2020].
8. D. R. Staff, “vulnerabilities-threats 71% of Security Pros See Threats Jump Since COVID-19 Outbreak,” 7 April 2020. [Online]. Available: https://www.darkreading.com/vulnerabilities---threats/71--of-security-pros-see-threats-jump-since-covid-19-outbreak/d/d-id/1337498?fbclid=IwAR3N8EF83CPJW89Z1u2RtIwpIjmAEVsJSKGwqAJvMdjGWjvi-DJyJLSekIc. [Accessed 9 April 2020].
9. D. M. &. L. Kelion, “Coronavirus: Call for apps to get fake Covid-19 news button,” BBC NEWS, 9 April 2020. [Online]. Available: https://www.bbc.co.uk/news/technology-52157202. [Accessed 9 April 2020].
10. D. A. Fauci, “Coronavirus update: In the cyber world, the graph has yet to flatten,” 28 March 2020. [Online]. Available: https://blog.checkpoint.com/2020/04/02/coronavirus-update-in-the-cyber-world-the-graph-has-yet-to-flatten/. [Accessed 5 April 2020].
11. J. Chadwick, “Explosion in cybercrime targeting Netflix users detected since the coronavirus outbreak with hundreds of phishing schemes and fraudulent websites set up to trick viewers,” Associated Newspaper Ltd, 15 April 2020. [Online]. Available: https://www.dailymail.co.uk/sciencetech/article-8221407/Netflix-users-targeted-cybercriminals-COVID-outbreak.html. [Accessed 16 April 2020].
12. A. Hamacher, “Coronavirus is driving drug users to the dark web and Bitcoin,” Chainalysis, 1 April 2020. [Online]. Available: https://decrypt.co/24193/coronavirus-is-driving-drug-users-to-the-dark-web-and-bitcoin. [Accessed 20 April 2020].
13. National Cyber Security Centre & Cybersecurity Infrastructure Security Agency, “Advisory: COVID-19 exploited by malicious cyber actors,” 8 April 2020.
14. Endsley, M.R.: Toward a Theory of Situation Awareness in Dynamic Systems. Human Factors Journal 37(1), 32-64. March 1995 DOI: 10.1518/001872095779049543