Klover Multidisciplinary Journal of Engineering
Volume 11 Issue 4, October-December 2023
ISSN: 2995-4118
Impact Factor: 7.36
http://kloverjournals.org/journals/index.php/Engineering

DIGITAL DEFENDERS: THE COVID-19 CATALYST IN CYBERSECURITY EVOLUTION

Kwame Adu, Emmanuel Osei Agyemang
Koforidua Technical University, Koforidua, Ghana

Abstract
The outbreak of COVID-19 in late 2019 and its subsequent declaration as a pandemic by the World Health Organization in 2020 have had a profound impact on societies worldwide. As the world adjusted to the "new normal," discussions surrounding the coronavirus family and its effects became prevalent globally. This paper aims to explore the far-reaching consequences of COVID-19 on cybersecurity. With governments implementing physical distancing regulations and imposing lockdowns to mitigate the spread of the virus, the first wave of infections prompted a surge in cyber threats. Ghana, for example, enforced a month-long lockdown in its capital city due to a rapid increase in cases. The primary focus of this study is to investigate the realm of cybersecurity and analyze the influence of COVID-19 on this domain.
During the ongoing second wave of the pandemic, there is significant uncertainty among the general public, with an abundance of both accurate and fake news circulating. Corporations are seizing the opportunity to advance their agendas, while cybercriminals seek to exploit the pandemic for personal gain. This paper examines the current threats faced by internet users and provides guidelines to mitigate these imminent risks. As society has adapted to the "new normal," cybersecurity experts have assumed the responsibility of safeguarding the public, as cybersecurity is now considered a public service. Consequently, there has been a surge in daily cybersecurity attacks targeting the general population. However, public awareness and vigilance regarding cybersecurity remain inadequate. Therefore, there is an urgent need to educate the general public on fundamental cybersecurity principles to enable them to protect themselves against various cyber threats.
Furthermore, this paper explores the broader impact of COVID-19 on individuals, businesses, and the economy from a cybersecurity perspective. It emphasizes the pressing requirement for cybersecurity education and awareness in light of the pandemic's significance. The COVID-19 crisis has underscored the utmost importance of cybersecurity in safeguarding society's well-being and highlights the need for comprehensive measures to combat cyber threats effectively.

Keywords: COVID-19, pandemic, cybersecurity, cyber threats, public awareness, lockdown, physical distancing, fake news, cybercriminals, education, society.

Introduction

COVID-19 has had an enormous effect on the regular routines of the world bringing about the new normal. Discussions regarding how the family of coronavirus is impacting our lives in more ways than one and how it's one of the most commented topics worldwide. COVID-19 has had a huge impact on the world since it sprung in the latter months of 2019. In December of the year 2019, the first active case of the virus was identified in Wuhan, Hubei, China. Later in March of the year 2020, the virus was declared a pandemic by the World Health Organization. It brought an era of mass hysteria and confusion alongside a massive number of infections across the world. When the COVID-19 outbreak

began, several countries immediately implemented physical distancing regulations. This write-up explores the impact of COVID-19 on cybersecurity [1]. Due to the huge number of infections during the first wave, most government leaders and society heads put entire countries and organizations on lockdown. Due to the number of cases that rapidly increased in the nation's capital of Ghana, it was lockdown for almost a month to contain the virus and decrease the spread. The main scope of this paper is to explore the realm of cybersecurity and the impact COVID-19 has had on it. Amidst the second phase also popularly called the second wave of the COVID-19 pandemic there is currently massive uncertainty amongst the general public on what is accurate news and what is fake news. There are also corporations trying to push their agenda, amidst this hysteria, whilst cybercriminals are trying to profiteer out of this pandemic. This paper explores what current threats that internet users face, guidelines on how to alleviate such imminent threats. Currently, the pandemic is a part of the new normal of society so people have made up their minds to just stay safe and adhere to protocols to help them finesse the virus. Cybersecurity experts due to the current situation are now faced with the task of protecting the population in general since they are a public service. There is currently a huge cybersecurity attack inflow being launched daily against the general public. Cybersecurity vigilance is still massively lacking in the general public and there is a need for educating the general public on the fundamentals of cybersecurity to enable them to protect themselves against cyber threats of all kinds. This paper also looks into the impact that COVID-19 had on the population in general, businesses/organizations, the economy from the cybersecurity perspective, the imminent requirement of cybersecurity education awareness, as it has gained utmost importance.

1 Background

At the time this study was done, the virus has been around for more than a year. The World Health Organization identified coronaviruses (CoV) as a big family of viruses that can cause a variety of illnesses, ranging from the common cold up to the more severe illness named Severe Acute Respiratory Syndrome (SARS-CoV). The exact disease that was identified as the pandemic is the Coronavirus disease (COVID-19) which is a new strain in the CoV family. The World Health Organization identified Severe Acute Respiratory Syndrome Coronavirus 2 (SARS-CoV-2) as the virus that is responsible for causing the COVID-19 [2]. The WHO clarified clearly that the correct disease classification for the pandemic is COVID-19 which clarified the two different names floating around in the media. There are other pandemics ongoing with regards to Middle East Respiratory Syndrome (MERS) and HIV/AIDS. Ebola was the most recent pandemic deemed as being under control initially in Africa [3]. The term under Control in this instance means there is no crisis seen in recent times and that the virus is under wraps. Ebola cases are still active and the last outbreak was recorded in August 2018. The last confirmed case of Ebola was recorded in the year 2020 in February, and the classification of under control can still be used here. There have been pandemics that killed several millions of people, such as the Bubonic Plague, Small Pox, and the Spanish Flu. The difference between the previous pandemics is that there was much more isolated impact and far less global impact, due to communication across the globe being significantly less prevalent and traveling vast distances being uncommon. There have been several detailed images depicting a summary of the pandemics during the past few months in a very well-

structured manner. The Ghana health service provides daily updates with regards to COVID-19 cases throughout the country. Several cybersecurity threats broke out during the outbreak of Ebola [4]. The same consequences are still being suffered now, as that we had during the Ebola outbreak. The only positive thing we had during the Ebola period was that most isolated cases were in the West African region, and did not spread globally as the coronavirus has. Although Ebola is deemed under control, people are told to stay vigilant as there is no mention that the outbreaks are over. The same trajectory can potentially be said for the COVID-19 outbreak in the upcoming years, for many years to come, cybersecurity threats will not be a thing of the past. Over 53 billion USD has been lost in both social and economic sectors in West Africa in the battle against Ebola [5].

Similarly, With SARS having a 10% fatality rate, MERS 35% with COVID-19 2.2%current statistics show that Severe Acute Respiratory Syndrome (SARS) and MERS have a much higher fatality rate [6]. The infection rate of COVID-19 is however much quicker when compared to SARS and MERS. It took only 48 days for the first COVID-19 infection, 903 days for MERS to affect the first 1000 people, and took 130 days for SARS [3][2].

2 The issue of social engineering

In a world filled with fear and the need to stay informed on issues regarding the times, cybercriminals have been provided with a stage of unsuspecting victims they can prey on. Social engineering is preying on individuals who are at a heightened emotional state at its peak in this time. Social engineering is the science of using social interaction as a means of persuading individuals or organizations to conform with a specific request from an attacker where a computer is involved in either the social interaction, the persuasion, or the request [4].

The human element is the glitch or vulnerable element within security systems. Unfortunately, it is the basic characteristics of human nature that make people vulnerable to the techniques used by social engineers to exploit various psychological vulnerabilities to manipulate the individual to disclose the requested information. Lately, most organizations make their workforce work from home where it is possible. Most countries have gone into full lockdown because of the second wave forcing everyone to stay indoors. Now people are fully reliant on technology for communication, news, entertainment, and social interaction. Reasons, why individuals are vulnerable or at the mercy of these social engineers, is because;

- Almost every country has massive reliance on online connectivity and network infrastructure.
- Working from home has not been fully trailed by all organizations before.
- Individuals who are not necessarily inclined when to tech have now suddenly become accustomed to using technology for their daily lives.
- In times of uncertainty, the human mind becomes very curious.
- Society is spending most of its time-consuming online services, which in turn could lead to riskier behavior.

The above-stated factors have caused a massive rise in cyber-attacks. Some of the typical cyber-attacks have also moved over to the physical realm where criminals are using social engineering techniques to

infiltrate people's houses. Followed by this are social engineering techniques utilized within this new cyber-security threat era due to the circumstances at hand.

2.1 Fake URL's as a social engineering technique

The past months of the coronavirus pandemic have brought about a massive increase in the procurement of fake URLs, associated with COVID-19. Typically, the mode of operation is for scammers to scoop up a bunch of COVID-19 related domains, and to turn them into malicious malware injection sites. After all of the domains are taken, the scammers will eventually start preying on the domains containing typos, using words like 'coronavirus' instead of 'coronavirus'. The excerpt of the domain names that have been registered from 1st to the 2nd of March 2020, that include the name corona are as follows; corona-crisis.com, corona-emergency.com, combatcorona. com, buycoronavirusfacemasks.com, beatingcorona.com, coronadetection.com, and coronadatabase.com [7].

This clearly shows that this process is continuously ongoing and that people should be on the lookout for fake URLs. It is unfortunate that in such a mass hysteria situation, good URLs, such as 'beating corona' or 'corona detection', have already been taken over by individuals with malicious intent. These URLs could have been used for good purposes, allowing people to easily locate the correct and accurate information.

2.2 Phishing as a social engineering technique

Phishing is one item that has seen a massive rise during this coronavirus era. Society has become hungrier for information, or even for some form of relief, and thus phishing is just so much more successful during these times. Most of the examples that have been witnessed in the wild are e-mails, such as from tax authorities offering victims tax refunds to help them cope with the coronavirus pandemic. All they had to do was enter their name, address, phone number, mother's maiden name, and bank card number a total scam [8].

Cyber attackers are also very closely following global trends and news. The latest phishing scam that occurred is regarding the 1000 USD to that United States might offer to each household for relief during these difficult times.

2.3 Physical attacks

People often forget the physical attacks that still take place when talking about the cybersecurity threat. These types of attacks still rely on social engineering. They are usually based upon the mere fact that people are already in a state of hysteria and need the assistance of some kind. There have been reported cases within South Africa where this is an active problem. One matter has been reported by one of the physical security agencies, that individuals are posing good citizens and offering people free face masks, hand sanitizer, and other products whose supplies have been stretched thin during the coronavirus crisis. Using this technique, the "good citizens", are gaining physical access to victims' households. The other technique is individuals posing as people who can help to assist to disinfect your household. These individuals then request access to your home, as they need to spray chemicals in the house and ask you to wait outside whilst this process is happening.

In both these cases, the cybercriminals are preying on the notion that people are in fear and have the inherent need to stay safe. The notion of staying safe currently, is to use cleaning products and to ensure your home is clean.

2.4 Extortion and scam

A massive rise in individuals starting up donation webpages where people can donate to aid researchers in finding the cure for COVID-19 has also been initiated. People are inherently good and always want to assist, and thus social engineers are preying on the mere fact that people want to assist their fellow countrymen by donating to the cause. In most of these cases, these donation pages are not correctly managed and typically only the individual hosting the donation is profiting from the donation drive. There have been several examples of this in the wild. One of the worst ones in the past month is where almost 2 million USD was stolen through cryptocurrency donation scams. The attackers were smart in the sense that they asked the victims to donate in bitcoins, as it is almost impossible to trace where the money ends up eventually.

2.5 Spreading misinformation as a social engineering tool

Misinformation is one of the biggest enemies of society during this pandemic. Since the public themselves are doing a spectacular job by sharing sensational fake news amongst one another, cybercriminals are only required to publish the news sensationally. There has been a massive influx of fake news articles and several companies are actively trying to resolve this. The Humanitarian-to-Humanitarian (H2H) Network has invested 500 000 GBP to fight against misinformation. It has reached the point where the government had to step in and the South African government has placed a legal requirement to not spread fake news. It has been made a criminal offense according to a government gazette that has been released on the 18th of March 2020.

The excerpt from the government gazette reads as follows:

- Any person who publishes any statement, through any medium, including social media, to deceive any other person about COVID-19.
- COVID-19 infection status of any person.
- Measures taken by the Government to address COVID-19 commit an offense and are liable on conviction to a fine or imprisonment for a period not exceeding six months, or both such fine and imprisonment.

Several of these fake news websites, also require users to register to view the news, and thus the attack can obtain personal information from the individual. Downloading malicious software is another method of how attackers attempt to steal information with emails having download links with Safety measures.

2.6 Spreading personal agendas as a social engineering technique

It is of utmost concern that it is currently one of the best times to push a personal agenda during these trying times. Several individuals are trying to profit from this by stockpiling products and eventually trying to resell the products at a much higher value. Fortunately, several governments have put a stop to this, and price gouging has been forbidden by law. Governments are also stepping in against individuals who are trying to push their products. Formidable steps are being taken against individuals;

however, it is still only after the fact that governments have identified the problem and have stepped in. Fortunately, governments have stopped individuals from profiteering during this pandemic, it is very difficult to stop organizations from doing the same.

One of the biggest questions currently is whether ibuprofen can worsen your COVID-19 condition. There was a tweet by Olivier Veran, who is a neurologist at the Grenoble-Alpes University Hospital, that made a bold claim that ibuprofen can worsen your condition, which was backed by an article by Lancet [9]. After this statement has been, both the Food and Drug Administration (FDA) and the European Medicine Association invalidated these claims by saying there is no scientific backing to this claim at the current stage [10].

2.7 Malicious websites

One of the very first cyber-attacks related to COVID-19 was regarding the fake COVID-19 maps. Johns Hopkins University provided one of the very first maps which included statistics to the world. This has been a great resource to society and has proven to be massively beneficial. However, since it was so popular, cyber attackers made their fake versions of the website that required you to download a plugin and showed just how convincing the fake pages can appear. This plugin would then in turn allow an attacker to gain remote access to your system.

In another example, there have been websites masquerading as the official communication channels, such as the WHO or Center for Disease Control (CDC), and asking recipients to download documents containing safety tips. It has later been found that most of these malicious websites, and the files that were subsequently downloaded, contained malware designed to steal banking credentials or to key log people's passwords [7].

3 Impact and prevention

COVID-19 has already had a massive impact on the world. Society will most likely never be the same after this, however, we can use the knowledge obtained throughout the pandemic for a better future. Society, unfortunately, does not always respond to any warnings, as there is typically a reluctant attitude towards warning signs.

The COVID-19 pandemic will have the largest impact in the following areas:

• **Businesses** • Employees are less secure in their home environments as all the company firewalls are not in place to protect them.

• All individuals are forced to embrace technology, it is almost assumed that everyone has the required technical skills.

• The business has to suddenly implement work from home policies, something they were not prepared for at all.

• Large corporations' VPNs cannot handle the load to access the network thus minimizing productivity while working from their home environment.

•Economy

• Stock market crashes lead to a massive financial loss to both businesses and individuals.

• Interruption to businesses causes a massive strain on the economy. Country leaders have to make far-reaching decisions, in short periods that can have long-lasting impacts.

- Fighting economic impact by reducing interest rates [11].

Financial losses seem to be one of the major trends of the impact of COVID-19 in society, from a general perspective. Travel has become a sector that has been hit extremely hard with travel bans in effect with the airline revenue losses. These economic effects have also been felt with stock prices, oil, and bitcoin prices all having drastic devaluation. More specifically, could we have been better prepared for the change in the economy and cybersecurity threats. Unfortunately, and sadly so, the cybersecurity threat landscape has not changed due to the outbreak of COVID-19 [12]. There are several organizations out there that are continuously providing society with ways they can protect themselves. Their advice to individuals is centered on the following;

- Watch out for shortened links.
- Be wary of emails asking for confidential information.
- Only download files from trusted websites.
- Using the right coronavirus map;
- Make sure you donate to the right place if you feel the need to donate.
- Carefully examine any URL or email address you see.

•Misinformation

- Misinformation has caused a reasonable time wastage.
- It takes a massive amount of mental effort to correct information where people already believe the incorrect versions;
- Decision-makers have to make uninformed decisions, as not all information can be trusted.
- Inaccurate information has a more negative impact than having no information at all.

4 Conclusion

It will take years for the world to recover from the COVID-19 pandemic. COVID-19 has brought massive bouts of mass hysteria, panic, and confusion. All of the mentioned items have had a massive impact on the mental state of individuals and the cybersecurity threat transformed massively, almost overnight. There was a significant increase in cybersecurity attacks as leaders were poised to make tough decisions on the future of their countries. Society was unsure of what was happening at this time and unsure how to react and the cybercriminals took this opportunity to strike. This study elaborated on the impact COVID-19 has had on cybersecurity. Cybersecurity awareness is something that is still massively lacking in society, and unfortunately, society has now been forced to be more vigilant. The time is now to focus on cybersecurity education, as it is right now where it is most needed. Organizations need to start investing in their workforce now, as the risk to the organization has significantly increased. The workforce is no longer behind the organization's firewalls, each employee is only behind their home router, with limited to no security. People need to be vigilant, however, we require organizations to educate their workforce to protect themselves.

5 References

H. Noprisson, "A Survey of the Online Learning Implementation During COVID-19 Outbreak," *International Journal of Recent Contributions from Engineering, Science & IT*

(iJES), vol. 8, no. 4, p. 18, 2020. https://doi.org/10.3991/ijes.v8i4.17913

WHO, "SARS (Severe Acute Respiratory Syndrome)." [Online]. Available: https://www.who.int/ith/diseases/sars/en/. [Accessed: 14-Jun-2021].

WHO, "Middle East Respiratory Syndrome Coronavirus (MERS-CoV)." [Online]. Available: https://www.who.int/csr/don/24-february-2020-mers-saudi-arabia/en/. [Accessed: 25-May-2021].

Trend M, "Social Engineering Watch: Ebola Virus Being Used as Bait to Lure Victims." [Online]. Available: https://www.trendmicro.com/vinfo/tr/security/news/cybercrime-and-digital-threats/social-engineeringebola-virus-being-used-to-lure-victims. [Accessed: 15-Jun-2021].

Sirleaf E. & Panjabi R, "Five Key Lessons from Ebola." [Online]. Available: https://time.com/5806459/five-key-lessons-from-ebola-that-can-help-uswin-against-coronavirus-everywhere. [Accessed: 12-Oct-2021].

Y. Liu, A. A. Gayle, A. Wilder-Smith, and J. Rocklöv, "The Reproductive Number of COVID-19 Is Higher Compared to SARS Coronavirus," *Journal of Travel Medicine*, vol. 27, no. 2, 2020. https://doi.org/10.1093/jtm/taaa021

Christie M, "Online Scammers Target Vulnerable Internet Users During Coronavirus Outbreaks." [Online]. Available: https://abcnews.go.com/US/online-scammers-target- vulnerable-internet-users-coronavirusoutbreak/story?id=69675134. [Accessed: 12-Oct-2021].

Fowler H. & Duncan C, "Hackers Made Their Coronavirus Map to Spread Malware, Feds Warn." [Online]. Available: https://www.miamiherald.com/news/nationworld/national/article241171546.html. [Accessed: 20-Sep-2021].

F. and D. Administration, "No TitleFDA Advises Patients on the Use of Nonsteroidal Anti-Inflammatory Drugs (NSAIDs) for COVID-19." [Online]. Available: https://www.fda. gov/drugs/drug-safety-and-availability/fdaadvises-patients-use-non-steroidal-anti-inflammatory-drugs-nsaidscovid-19?mod=article inline. [Accessed: 11-Oct-2021].

Kolata G, "Is Ibuprofen Really Risky for Coronavirus Patients?" [Online]. Available: https://www.nytimes.com/2020/03/17/health/coronavirusibuprofen.html

Sillers J, "Coronavirus: Bank of England Cuts Interest Rates Again." [Online]. Available: https://news.sky.com/story/coronavirusbank-of-england-cuts-base-rate-to-0-1-11960336. [Accessed: 23-Jun-2021].

Simpson M, "Interest Rate Cut for SA Seems Likely Due to Coronavirus Crash." [Online]. Available: https://www.thesouthafrican.com/news/finance/