COVID-19 PANDEMIC - CYBERCRIMES VS CYBERSECURITY

Pritish Kumar Bhoi[1], Tripti Dhote[2]

[1,2] Symbiosis Institute of Digital and Telecom Management, Symbiosis International (Deemed University), Pune, India.
Email: [2]tdhote@sidtm.edu.in

Abstract

The whole world as we know is experiencing the worst ever pandemic in the history of mankind. The novel Corona Virus i: e COVID-19 has shaken the world economy to its knee. With the rapid spread of the virus, lots of tech giant companies are busy workings with the Govt. to handle the situation. As most people are accessing confidential data through home routers, hackers are easily finding the loopholes to get to the systems and do mischief things. The paper tries to investigate the current scenario of COVID 19 and how it has become the catalyst for the cyberwar between hackers and cybersecurity specialists. This paper will go through various ongoing use instances of cybercrime examining differences from the previous pandemics. It also aims at realizing the relevance for cyber security in the current context along with basic guidelines against cyber threats.

Key words: Cybercrime, Cyber security, COVID-19, Awareness & Education.

Introduction

The world is always subjected to change and the people are bound to adopt in according to the time. To these changes, every individual has a unique response. But this time, the change is quite different as the cause of change is an epidemic; COVID-19 which itself has lots of negative impacts. The journey of coronavirus from its origin to being the deadliest one has brought along political, medical, and economical discussions about the COVID-19 families. The World Health Organization (WHO); on 11 March 2020, declared novel COVID-19 as a pandemic due to its massive impact worldwide.

As the infection increases rapidly around the world, it has lead people toward the era of confusion and hysteria, as result to this has prompted the extreme change in digital crime on the web. The paper aims to explore and focus on the influence of COVID-19 had within the sphere of cybersecurity being challenged by hackers. At present, there is a colossal measure of unconventionality among the individuals on what is fake and what's genuine. Some companies are trying to tackle the situation amidst this hysteria while cybercriminals are finding ways to exploits the situation through cyber-attacks.

The time at which this paper has been written will allow the reader to explore through the current threats that are the hackers are throwing at the table and how the cybersecurity specialist is doing to prevent it. The paper also alleviates the basic guideline that the general public should do to increase their defense in the system. It also contains a predicting future depending upon the current scenarios and upcoming situations.

Since the whole world is racing toward finding the perfect vaccine for the COVID-19, predicting the world's economy and how it will impact the technology field in the future would be a tough task.

Within these 6 months of the ongoing pandemic, the responsibilities lie with the cybersecurity specialists to provide the utmost protection to the public as a public service. Currently, there has been an enormous amount of cyber-attacks across different continents and there is no end to it. So something needs to be done about it. But due to the lack of education in cybersecurity amongst the techies as well as the general public, cyber-criminal currently is a major problem in the field of technology and advancement, as nobody was prepared for this COVID 19 epidemic.

The second part is a quick review of how the recent pandemic COVID 19 has been different from the previous pandemics and what are the similarities associated with it. The third part will dive into mentioning different cyber-related use cases that are occurring and how they are different from the past. Forth part will be targeted towards the impact of COVID 19 on business, economy, technologies, and the public from the Cybersecurity perspective. It will also emphasize education and awareness related to Cyber threats and how they can be prevented. The last part will summarize the whole paper and will discuss the possible outcome in the future.

Objective

From a current pandemic perspective, the objective of this research paper is to examine the impact of cybercrime due to different type of anonymous cyber threats and attacks, that the world is experiencing globally amid COVID 19. Here the current changing threat landscape for the employees and the general public has been analyzed, showing how people are now highly exposed to the digital worlds and how they can be easily fooled by the different cyber-attacks in the name of the pandemic relief campaign due to lack of awareness of news & low-security measures. This paper also gives a detailed guideline about the new security norm that the general public can learn and follow and can avoid the data breach of their personal & organizational data.

Literature Review-

Numerous Pandemic like severe acute respiratory syndrome (SARs), dengue, smallpox, cholera, HIV, etc. had taken place in the past which had led to the devastation of the humankind. One of the deadly pandemics was the flu pandemic which the world still sees it as a disease that never left the society. For Instance, one of the most death records that have been recorded by any disease is the flu, which had been declared as the pandemic in the year 1918-1919.

But the pandemics that occurred in the past were very much restricted to their areas of origin due to large communication and transport gaps around the world. The pandemics were significantly prevented and hence were less impacted by the world economy [1].

There is no active case right now except the COVID 19. Ebola is one of the deadly pandemics that that world has seen in recent times. The researchers were able to control the virus to a great extend though it can be said that the Ebola is not completed erased from the world but had been controlled through medication. There have been some Ebola active cases detected on 17th February 2020 but WHO classified that virus is under control [2].

At the time of writing this paper, the COVID 19 pandemic has already crossed 5 months and yet researchers are struggling to find the perfect cure for the novel COVID 19. Researchers are fitting together unique pieces and trying their best to develop the vaccine [2].

From the common cold to the more severe illness named MARs-COV or SARs-COV, the whole bunch of the coronavirus has been classified according to their severity level by World Health Organization which have recently declared worldwide that the correct name of this disease is COVID-19 [3].

Dengue was one of the major diseases which was declared as a pandemic in recent times. Several developing countries had faced the brutal wrath of this fatal form of the Dengue [1], [4]. Among this the most severe form of dengue had taken place in Latin America in the year 2015 – 2016.In May 2015, Brazil had recorded the 1st ever cases of the Dengue which triggered a pandemic and reach up to 1.5 million active cases during that time in the month of December 2015.And by March 2016 more than 34 countries had been affected by this disease [5].

It made a significant impact on the world’s economy through high profile cyber breaches. For e.g. by the end of 2015, there was a security breach in Sony PlayStation Entertainment (SPE) by a hacker group calling itself Guardians of Peace, or GOP steeling 100TB of user’s data by that time [6].

Unfortunately, Cyber threats had also increased due to the outbreak of Ebola [7]. The current pandemic is also showing the same trend as it was showing for the Ebola outbreak. The good news about the incident we have during Ebola was that it was isolated & generally separated toward the Western region of Africa, and unlike COVID 19 it was not able to spread across major countries [8].

Cyber threats are increasing day by day as more people are working from home and with less secure networks. More than 53bn dollars of the world's economy had been impacted by the Ebola outbreak which in turn had affected the people socially and as well as mentally

For COVID 19 pandemic this figure will be tenfold times more in upcoming months and cybersecurity specialists have to come up with a new strategy to prevent the recent and upcoming attacks [9].

Currently, the novel COVID 19 which has a fatality rate of 2.2% w.r.t the Middle East Respiratory Syndrome having a fatality rate of 35% and Severe Acute Respiratory Syndrome having a fatality rate of 10% [10]. The frequency at which the COVID 19 has been infecting the people is much higher as compared to MARs & SARs. It took just 48 days for the COVID 19 cases to reach the first 1000 people whereas for MERS it took 903 days and for SARs it took around 130 days [11].

The annual GDP of Southeast Asia & China took a major blow due to the increased cases of the SARs which in turn had declined the GDP by 1% & 0.5% respectively [12]. Mouton F have estimated a salary loss of 12.3-28.4 billion USD for East and Southeast Asia during the SARS outbreak in 2003 [13].

A few areas of the economy might be more intensely influenced than others. For instance, it is estimated that if travelling will be cut down on for US residents due to outbreak then for airline industries the loss was approximately around 19% of 8bn dollars [13].

Thus, there will always be long term damage on the economy due to the occurrences of any pandemic [13]. The ineffective screening process of the passenger in airports during the SARs pandemic has also led to the economical and psychological decline in the year 2003 [14].

Research Methodology

The study actually uses the approach of literature review methodology which uses different sources describing different types of similar events and incidents that had occurred during the past pandemics. The study also tries to differentiate, how the COVID-19 pandemic and its impacts have been different from earlier one in terms of cybersecurity, cyber awareness, way of working business, etc. It also analyses the different cyber risk that the general public and organization were falling into through different fake COVID-19 campaign set up by the attackers to lure the users. The overall secondary research has been obtained by referring to different databases: Scopus, Emerald Insights, & Research Gate. Additional data has been obtained from different search engines like google, yahoo using keywords like COVID-19, Cybercrimes, Landscape of Cyber Security Threat, Cyber Security awareness & education, Cybersecurity.

The Landscape of Cyber Security Threat

When panic is thriving and the feeling of being informed by any means or source, it provides hackers a huge platform of unsuspecting victims. Social engineering is preying on those people who are in mental or emotional depression or the individual who lacks the use of technology [15]. Social engineering is defined as "the science of using social interaction as a means to persuade an individual or an organization to comply with a specific request from an attacker where the social interaction, the persuasion or the request involves a computer-related entity". As clearly stated by various authors the human element is the 'glitch' or vulnerable element within security systems [16]. A lot of people are fascinated by the technique used in social engineering as they get easily exploited due to psychological vulnerabilities thus disclosing information. As most of the people are working from home now, they are using the technologies fluently both for news, communication, social, and entertainment [13], [17]. According to the authors, the major factors that contribute to the increase of the cybersecurity threat landscape are as follows.

- High dependency on society due to digital infrastructure.
- Organizations have never implemented the full work from home concept earlier.
- The high dependency on online connectivity and consistency due to a high surge in VM & online platforms.
- Especially in times of uncertainty human psyche can be very a mystery.
- Hackers are active as more and more audiences are online on the internet.
- Individuals who are not 'tech-savvy' are bound to adopt some technologies for their daily needs.

All this key factor leading to a massive increase in cyber-attacks.

Phishing

Phishing is one of the most popular attacks that have been growing like an insect in this digital era due to Covid19 Situations. A single phishing mail can be so effective that it can take down a whole organization by implementing malware in it. For example, fake specialists offering "large discounts" to assist them with adapting to the coronavirus pandemic. The most recent phishing trick that happened is receiving mail from US govt. stating "1000 USD offering to each household for improvement during these troublesome occasions" [15].

There has been a sudden increase in counterfeit URLs which are related to COVID 19. A simple technique used by the attacker is that they gather a lot of info about the COVID 19 and try to transform it into a malignant malware infusion locale.

Different sites have been acting as a real web page to attract the users e.g. [18].

– coronacombat.com

– buycoronavirusfacemasks.com

– coronadatabase.com

As many people are in house and searching for the methods to get rid of the corona, they are easily being targeted by clicking on the fake URLs acting as a real one thus helping the attackers to locate the user locations and info [18].

Preying on the good of people

People shows lot of kindness when it comes to donation, the same case is additionally occurring during the pandemic as more and more occupants are attempting to go through some cash for the honorable purposes like donating patients or individuals some money who have been influenced because of employment misfortune. Here social engineering assumes a major job when we slanted the entire circumstance in terms of the cyber-attacks [19]. Programmers are effectively ready to clone a legislature based site page and afterward can request donations for noble cause. What's more, when any charity has been done through that page the cash consistently remains with the person's facilitating the page. There have been a few instances of this in present. One of the most noticeably terrible ones in the previous month is the place where just about 2 million USD was taken through digital currency gift tricks. The attackers were shrewd as they requested the casualties to give in bitcoins, as it is practically difficult to truly follow where the cash winds up unescapably [19].

Impact & Prevention

Some Other Key factors and changes during the pandemics: -

Misinformation

- Wrong data has a more negative effect than having no data by any means.
- Leaders need to settle on clueless choices, as not all data can be trusted

- It requires a huge measure of mental exertion to address info where individuals as of now had accepted the incorrect adjustments.
- Deception on information has led to wastage of gigantic measure of time

Businesses

- Business needs to out of nowhere execute telecommute approaches like work from home, something they were not set up for by any stretch of the imagination
- For some representatives, the security level is less in their home surroundings as firewalls are not set by their organization to ensure them
- All people are compelled to grasp technology, it is nearly accepted that everybody has the necessary technical aptitudes.
- Companies VPNs can't deal with the heap to get to the network and hence limiting profitability while working from their home condition.

Fear Mongering

- People don't trust the administration on the security of an uninterrupted supply of necessities from supermarkets, which led to panic and bulk buying.
- The mandatory needs of testing for COVID-19 for every individual have increased the pressure on the clinical institute.
- Cancellation of flights, trains, or other sources of travel has increased the individual uncertainty of returning their native place or nation of origin, which eventually gives a feeling of abundance.

Economy

- Economy slowdown had pushed lot of organization to standstill position;
- Nation pioneers need to settle on extensive choices, in brief timeframes that can have enduring effects; for example, dropping off their interest fee by 0.5% in the UK and 1% in South Africa [19], [20].
- Securities exchange crashes lead to huge money related misfortunes to both individuals and large organizations.
- Battling COVID 19 had a financial impact which in turn leads to reduced loan costs.

Monetary misfortunes are by all accounts one of the significant impacts of COVID19 in the public arena, from a general point of view. The red flag in the movement has hit hard with the ban in travel in actuality with the carrier income misfortunes calculated approximately as 113 Billion USD [20]. Besides these, financial impacts have additionally been down with stock costs, oil, and bitcoin costs leading to radical degrading. The entirety of the negative effects that we have encountered, now prompts one query, are we ready for this? All the more explicitly, shall we be able to have been more readiness in the adjustment for digital security danger scene? Shockingly, and tragically along these lines, the digital security danger scene has not so much changed because of the epidemic of COVID-19. The main contrast presently is they have reformed to another "structure" or can be said as it has taken another account. The assaults which we have recently spoken about Ebola have only supplanted the word Ebola with the word COVID-19. Creators completely concur that out of nowhere there is a monstrous deluge of cybersecurity assaults, and this is absolutely obvious. The hackers are using this as bait during a pandemic for their benefit, and are also achieving great success. People are in an undermined enthusiastic state, subsequently; the digital risk had increased. People are as of now constantly under pressure which has a seriously pessimistic effect on their thinking ability. There are a few associations out there who are persistently giving society ways out so that they can ensure themselves safety. Every one of them has comparative headings, for example, the accompanying by Nord VPN and Cyber Reason [21].

Nord VPN

- Using the privilege coronavirus map;

- Prevent downloading anything and think cautiously before joining around;
- Better to keep a composed and calm mind;
- Make sure you give to the ideal spot; COVID-19: Impact on the Cyber Security Threat Landscape.;
- Analyze carefully any URL or email address you see.

Cyber Reason

- Watch out for unwanted pop-ups and abbreviated connections;
- Be careful about messages requesting classified data;
- Only download records from confided in site.

Conclusion

COVID-19 has conveyed alongside it monstrous scenes of widespread disorder and panic. These things greatly influenced the field of cybersecurity threats where people get affected mentally and financially. The rapid increase in cyber-attack not only impacted the organization but also put a great burden on the corporates in taking serious decisions on some mission-critical situations. Society was uncertain about how to react. The paper was very much inclined towards the impact and the cause that COVID-19 had on the cyber risk horizon that had shaken the world to a limit. This paper was composed as a preview in time, as every day this pandemic effect is taking a new turn and the impact of the cybersecurity risk scene is changing at a quick pace. It is from time to time like this the experts in the risk field need to get together and act on it, and this paper has given a glance at it. This paper shows us some of the majorly current security threats that the world is facing amidst COVID 19. The impact of COVID-19 was furthermore discussed and what kind of restriction can be imposed which can reduce its impact. Advanced security care is something that is still enormously weak in the open eye, and shockingly modern society does know how to go about it. Now is the perfect chance to focus on advanced security preparation. As the risk to the assets has been increased, organizations need to start placing assets into their workforce. The workforce is not anymore working behind the organization firewalls, each employee is simply behind their home router firewall, with limited security. People ought to be cautious, in any case, we anticipate that companies should train their workforce with the ultimate goal to make sure that they secure themselves..

References

1. Oi. Wing Ng and Y. Joo Tan, "Understanding bat SARS-like coronaviruses for the preparation of future coronavirus outbreaks — Implications for coronavirus vaccine development," Hum Vaccin Immunother, vol. 13, no. 1, pp. 186-189, 16 Sep 2016. [Online]. Available: https://doi.org/10.1080/21645515.2016.1228500. [Accessed 14 July 2020].

2. W. Markotter, "COVID-19: Why it matters that scientists continue their search for source of ‘patient zero’s’ infection," (2020, Mar 13). [Online]. Available: https://www.up.ac.za/news/post_2880755-covid-19-why-it-matters-that-scientists-continue-their-search-for-source-of-patient-zeros-infection-. [Accessed 14 July 2020].

3. A. Troncoso, "Zika threatens to become a huge worldwide pandemic," Asian Pacific Journal of Tropical Biomedicine, vol. 6, no. 6, pp. 3-6, 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2221169116302921. [Accessed 15 July 2020].

4. C. McLellan, "Cybersecurity in 2015: What to expect," (2015, Feb 5). [Online]. Available: https://www.zdnet.com/article/cybersecurity-in-2015-what-to-expect/. [Accessed 16 July 2020].

5. Trend Micro, "Social Engineering Watch: Ebola Virus Being Used as Bait to Lure Victims," (2014, Oct 20). [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/social-engineering-ebola-virus-being-used-to-lure-victims. [Accessed 16 July 2020].

6. A. Carmosino, "Background & History of the Coronavirus (COVID-19)," (2020, Apr 4). [Online]. Available: https://psychcentral.com/coronavirus/background-history-of-the-coronavirus-covid-19/. [Accessed 17 July 2020].

7. C. Huber, L. Finelli and W. Stevens, "The Economic and Social Burden of the 2014 Ebola Outbreak in West Africa," The Journal of Infectious Diseases, vol. 218, no. 5, pp. 698-704, 15 Dec 2018. [Online]. Available: https://doi.org/10.1093/infdis/jiy213. [Accessed 17 July 2020].

8. Cleanlink, "SARS-CoV-2 And COVID-19: What's The Difference?" (2020, Mar 10). [Online]. Available: https://www.cleanlink.com/news/article/SARS-CoV-2-And-COVID-19-Whats-The-Difference--25264. [Accessed 17 July 2020].

9. WEF, "3 charts that compare coronavirus to previous outbreaks," (2020, Feb 19). [Online]. Available: https://www.weforum.org/agenda/2020/02/comparing-outbreaks-coronavirus-mers-sars-health-epidemic/. [Accessed 18 July 2020].

10. M. Landis., "Pandemic Influenza: A Review. Population and Development Review," Research Gate, vol. 33, no. 3, pp. 429-451, 01 Sep 2007. [Online]. Available: https://doi.org/10.1111/j.1728-4457.2007.00179.x. [Accessed 18 July 2020].

11. J. W. Shega, P.D. Sunkara, A. Kotwal, P. Schumm and W. Dale, "Measuring Cognition: The Chicago Cognitive Function Measure in the National Social Life, Health and Aging Project, Wave 2," The Journals of Gerontology: Series B, vol. 69, no. 2, p. 66–176, 01 Nov 2014. [Online]. Available: https://doi.org/10.1093/geronb/gbu106. [Accessed 18 July 2020].

12. A. Rose, D. Wei and F. Prager, "Total Economic Consequences of an Influenza Outbreak in the United States," Publication of Society of Risk Analysis, vol. 37, no. 1, pp. 4-19, 23 Jan 2017. [Online]. Available: https://doi.org/10.1111/risa.12625. [Accessed 19 July 2020].

13. D. Gillen and W. Morrison, "Aviation security: Costing, pricing, finance and performance," Journal of Air Transport Management, vol. 48, no. 2, pp. 1-12, 13 Sep 2015. [Online]. Available: https://doi.org/10.1016/j.jairtraman.2014.12.005. [Accessed 19 July 2020].

14. R. Soni, "Social Engineering: The Science of Human Hacking,"(2020, May 22). [Online]. Available: https://medium.com/@OyeSoni/social-engineering-the-science-of-human-hacking-87ab39f85f24. [Accessed 20 July 2020].

15. A. Vishwanath, "What COVID-19 Teaches Us About Social Engineering,"(2020, Jun 11). [Online]. Available: https://www.darkreading.com/endpoint/what-covid-19-teaches-us-about-social-engineering/a/d-id/1337979. [Accessed 21 July 2020].

16. S. Morrison, "Coronavirus email scams are trying to cash in on your fear," (2020, Mar 5). [Online]. Available: https://www.vox.com/recode/2020/3/5/21164745/coronavirus-phishing-email-scams. [Accessed 24 July 2020].

17. K. Herrick, "How to Spot a Fake or Scam Website,"(2019, Dec 18). [Online]. Available: https://www.asecurelife.com/how-to-spot-a-fake-website/. [Accessed 25 July 2020].

18. M. Leonhardt, "Coronavirus $1,000 relief check plan not even final yet and experts say fraudsters are already looking to cash in,"(2020, Mar 19). [Online]. Available: https://www.cnbc.com/2020/03/19/what-to-know-about-scams-looking-to-cash-in-on-1000-dollar-covid-19-check.html. [Accessed 26 July 2020].

19. D. Nelson, "Thieves Swindle $2M from Coronavirus Preppers with Hand Sanitizer, Face Mask Scams," (2020, Mar 18). [Online]. Available: https://www.coindesk.com/thieves-swindle-2m-from-coronavirus-preppers-with-hand-sanitizer-face-mask-scams. [Accessed 28 July 2020].

20. J. Sillars, "Coronavirus: Bank of England cuts interest rates again and orders £200bn to be printed," (2020, Mar 18). [Online]. Available: https://news.sky.com/story/coronavirus-bank-of-england-cuts-base-rate-to-0-1-11960336. [Accessed 28 July 2020].

21. Cybereason Nocturnus, "Just Because You’re Home Doesn’t Mean You’re Safe," (2020, Mar 18). [Online]. Available: https://www.cybereason.com/blog/just-because-youre-home-doesnt-mean-youre-safe. [Accessed 30 July 2020].