International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958 (Online), Volume-9 Issue-4, April 2020

Cybersecurity Pros Warn – COVID-19 Pandemic as a Tool

Alex. R. Mathew

Abstract*: The COVID-19 pandemic has not only had health and economic implications on businesses, individuals, and governments but has also become a tool for hackers and crackers to use in committing cyberattacks. The purpose of this paper is to create awareness on the use of the pandemic as a cyberattack tool and to present remediation strategies. The research was conducted through a review of existing literature from websites and reputable databases, including Google Scholar and IEEE Xplore. The themes from the literature sources include the prevalence of phishing, scamming, spamming, and malware as the common attack vectors. Business enterprises, including operators in healthcare, finance, and Internet service provision, should actively implement risk management plans to monitor attack vectors and secure their systems, clients, and users from the COVID-19 attack tools.

Keywords*: COVID-19, cyberattack, tools, monitoring, protection, enterprise risk management.

I. INTRODUCTION

The world today currently generates huge amounts of data in various industries. Parhami [1] states that the daily generation date predicted for the 2020s will reach the yottabytes level up from the exabytes that were generated daily in the 2010s. For context, a yottabyte is 10^{24} bytes. Therefore, data is increasingly becoming of great value to the success of business enterprises and social ventures [2]. In the healthcare industry, for instance, the management of the volumes of data – through Big Data analytics – contributes to the improvement of people's conditions and the prevention of predictable medical issues [1]. There is, therefore, a major concern surrounding the integrity and the preservation of data, especially in healthcare environments. Attackers, also seek to exploit the large volumes of data for malicious purposes, including blackmail and monetary gains. One of the threat vectors that they are currently using to breach data in various organizations is the COVID-19 tool for cyberattacks. Business enterprises and individuals should, therefore, implement strategies to shield themselves from cyberattacks during the ongoing pandemic. This paper analyzes experts' warnings on the use of the COVID-19 cyberattack tool, especially in healthcare and finance settings and proposes methods through which organizations can shield themselves against these attacks.

Revised Manuscript Received on April 27, 2020.
* Correspondence Author
Alex. R. Mathe*, Ph.D.,Computer Science and Engineering (Cyber Security)

II. PROPOSED METHODOLOGY

The study explores the use of the literature review methodology. It uncovered that information by identifying online sources discussing the use of the COVID-19 cyberattack tool as well as journal articles, conference proceedings, and book chapters that discuss the countermeasures. The websites discuss the vectors through which attackers use information about COVID-19 to lure unsuspecting users and launch attacks against their systems and breach their data. These information sources were obtained from online searches on the Google search engine, Google Scholar, and IEEE Xplore databases using keywords such as COVID-19, cyber threat, cyberattack tool, countermeasures, and mitigation.

III. RESULT ANALYSIS

A. COVID-19 Cyber Attacks Tools

WebARX Security [3] reports that many threat actors have successfully used COVID-19 to craft malware and phishing attacks against unsuspecting individuals and institutions. The attackers have created a myriad of fake and dangerous websites that steal sensitive information from users through phishing. For instance, the New Delhi cybercrime division provided a list of fake links through which attackers perform such phishing. Based on these reports, WebARX [3] noted that the phishing attacks had increased by 350% since the outbreak of the pandemic.

Another vector that WebARX [3] reports is the use of phishing information that tell users that they are exposed to the novel coronavirus, and in the process deploy malware to the systems the targets are using. Other malware attacks are evident through malicious COVID-19 campaigns, the BlackWater malware masquerading as valid COVID-19 information, and the use of fake discount codes related to the virus [3]. Murray [6] reports that there are attackers who have inserted malware into mobile applications that are supposed to track the progress of COVID-19, with the apps having the ability to steal important information from the users [1].

Scams have also been on the rise during the pandemic, with respected authorities pointing out their prevalence during this period. According to the Federal Trade Commission [4], scammers take advantage of the fears and anxiety that people have related to the novel coronavirus, luring them into purchasing items that they do not need.

The attackers are also likely to commit financial fraud by sharing links to fake charity courses and donation platforms while spreading malware [5]. Furthermore,

KPMG reports that the attackers are using fake information and websites to channel traffic to their websites from where they can steal Office 365 credentials [7].

B. COVID-19 Cyber Attack Impacts

Various industries have suffered from the brunt of the COVID-19 cyberattack tool. Imperva Inc. [8] notes that even as the world grapples with the pandemic, news, foods and beverage, retail, gaming, law and government, and education industries have encountered spikes in traffic because of the services that they provide. However, the healthcare industry has witnessed a reduction in the amount of traffic [8]. Even then, attackers are still taking advantage of individuals seeking healthcare information by launching the phishing, scamming, and malware attacks.

Two of the sectors that are mostly affected by the wave of COVID-19 inspired cyberattacks are the healthcare and finance industries. The data breaches exploit pertinent health information and introduce financial losses to individuals and organizations [3]-[7]. Historically, the exploitation of health information has had negative impacts on both patients and healthcare organizations. Chernyshev [10] explains that the data breaches have opened doors for ransomware attacks, identity theft, and information-based financial losses. Moreover, the theft of vital patient information on sensitive medical data is a worrisome impact of data breaches [11]. Thus, the use of COVID-19 attack tools can introduce such challenges to healthcare institutions.

To individuals, the impacts might include the loss of sensitive information, identity theft, financial losses, and the loss of control over personal data. The impacts of the attacks on financial institutions are largely indirect because few attackers directly target financial institutions. The impacts include financial losses in theft and financial losses due to insurance claims on cyberterrorism [12].

C. Possible Control Measures

The most potent control measures revolve around the use of firewalls, authentication and encryption systems, and intensive training [9]. Chernyshev [10] explains the potential of digital forensics to the reduction of data breach incidents. The World Economic Forum (WEF) [13] explains that businesses can protect themselves from COVID-19 cyberattacks by providing end-point protection, using virtual private networks (VPN) for encryption, enforcing multifactor authentication, and using threat intelligence – a form of artificial intelligence (AI) to block breaches and malware attacks.

However, these methods work best for institutions that have IT infrastructure and the corresponding cybersecurity framework. For individual Internet users, the WEF [13] recommends the use of multifactor authentication, updated software and systems, secure their Wi-Fi access points, and become aware of the phishing, scamming, spamming, and malware that are propagated under the guise of COVID-19 information.

D. Software Tools

There are various tools that can help both businesses and individuals to shield themselves from the COVID-19 cyberattacks. These threat monitors include software tools such as Security Information and Management Systems (SIEM), Big Data Analytics, intrusion detection systems (IDS), and intrusion protection systems (IPS) [14]. Petrenko et al. [15] explain that these tools are a form of information protection techniques as they detect and prevent unauthorized access, viruses and malware, and information theft.

They achieve this daily monitoring by collecting security logs, incorporating IDS and SIEM rules in a fusion process, using cybersecurity intelligence to analyze trends, and specifying remediation strategies based on identified attack vectors from across the globe [16]. It is such processes that inspire watchdogs to identify current trends in the use of COVID-19 as a tool. The enabling technologies for the use of the monitoring tools include Big Data analytics, machine learning, and support vector machines (SVM) for intrusion detection and protection [17].

IV. DISCUSSION

A. The Threat of the COVID-19 Attack Tools

The major attack vectors that cybercriminals are using to launch attacks during the COVID-19 pandemic are phishing, malware, scamming, and spamming. Through the phishing and malware attacks, the hackers and crackers successfully use COVID-19 as a tool to breach users' confidential and sensitive data. The breach enables them to scam some individuals into purchasing unnecessary items related to the management of COVID-19, thereby leading to financial losses among users and the spread of unwanted items.

B. Recommendations for Combating the Attacks

The novelty of the attack vectors with the exploitation of COVID-19 calls for the education of individual Internet users. Various institutions, including the WEF, are already proactively educating users to beware of the scamming, phishing, spamming, and malware used during the pandemic [13]. The second recommendation is for Internet Service Providers (ISP) to play a role in protecting their subscribers from these attacks. It is the ISPs who have the capabilities of implementing the AI techniques of machine learning, knowledge acquisition, and SVM to protect the users from cyber threats [14].

All organizations which have an online presence should develop risk management solutions to combat the cyber threats that have come along with the COVID-19 pandemic. The enterprise risk management process should entail the identification, analysis, and prioritization of risks and threats using monitoring tools such as the SIEM software, Big Data analytics, IDS, and IPS systems. The next stage in the risk management process would be the development and evaluation of mitigation plans against the current pandemic-related threats. The systems that can help in this process include authentication, VPN, firewalls, encryption, and user education.

With the risk management plans in place, organizations and ISPs will be well-placed to combat the use of COVID-19 as a cyberattack tool. The most adversely affected industries – healthcare and finance – should actively deploy these monitoring tools during the pandemic. Since individual users might not have the capacity to install and run these solutions,

ISPs can weigh in and use them to monitor their networks and to shield their end-users from recognizable attack vectors during this pandemic. The ISPs also have the capacity to enhance data encryption to safeguard the information that users convey across various public networks.

V. CONCLUSION

Business enterprises and individuals should, therefore, implement strategies to shield themselves from cyberattacks during the ongoing pandemic. The reason is that attackers have utilized COVID-19 to launch phishing, scamming, spamming, and malware attacks on businesses and individuals. The best strategy for protecting organizations from this adverse event is the use of effective enterprise risk management plans that incorporate cybersecurity monitoring and remediation strategies. Central to the strategies are the techniques of Big Data analytics, IDS, IPS, and SVM for monitoring and analysis. The remediation procedures include authentication, encryption, the use of VPN, and the education of individual users.

REFERENCES

1. B. Parhami, "Data Longevity and Compatibility," in *Encyclopedia of Big Data Technologies*, Basel, Switzerland, Springer International Publishing AG, 2018, pp. 1-5.
2. S. Sabharwal, S. Gupta and K. Thirunavukkarasu, "Insight of big data analytics in healthcare industry," in *2016 International Conference on Computing, Communication and Automation (ICCCA)*, Noida, India, 2016.
3. WebARX, "COVID-19 Cyber Attacks," WebARX Security, 30 March 2020. [Online]. Available: https://www.webarxsecurity.com/COVID-19-cyber-attacks/.
4. Federal Trade Commission, "Scammers are taking advantage of fears surrounding the Coronavirus," FTC, March 2020. [Online]. Available: https://www.consumer.ftc.gov/features/coronavirus-scams-what-ftc-doing.
5. T. F. Duffy, "Cyber Threat Actors Expected to Leverage Coronavirus Outbreak," *Center for Internet Security*, vol. 15, no. 2, 2020.
6. A. Murray, "U.S. Attorney Andrew Murray Issues Warning For COVID-19 Scams," U.S. Department of Justice, Charlotte, NC, 2020.
7. G. Archibald, K. Robins and I. Gray, "COVID-19: Protect your team from phishing and cyber scams," KPMG, 26 March 2020. [Online]. Available: https://home.kpmg/au/en/home/insights/2020/03/coronavirus-COVID-19-phishing-cyber-scams-protection.html.
8. Imperva, "Imperva Research Labs Shows Significant Changes in Web Traffic During COVID-19 Pandemic," Imperva Inc. Research Lab, 26 March 2020. [Online]. Available: https://www.imperva.com/company/press_releases/imperva-research-labs-shows-significant-changes-in-web-traffic-during-covid-19-pandemic/.
9. W. Priestman, T. Anstis, I. Sebire, S. Sridharan and N. Sebire, "Phishing in healthcare organizations: Threats, mitigation and approaches," *BMJ Health & Care Informatics*, vol. 26, no. 1, 2019.
10. M. Chernyshev, S. Zeadally and Z. Baig, "Healthcare Data Breaches: Implications for Digital Forensic Readiness," *Journal of Medical Systems*, vol. 43, no. 7, 2019.
11. C. Murphy, "Healthcare Industry Held Hostage: Cyberattacks and the Effect on Healthcare Critical Infrastructure," ProQuest Dissertations Publishing, Ann Arbor, MI, 2017.
12. N. Tariq, "Impact of cyberattacks on financial institutions," *Journal of Internet Banking and Commerce*, vol. 23, no. 2, 2018.
13. World Economic Forum, "World Economic Forum Releases Guide on Protecting from Cyberattacks during COVID-19," Security Magazine, 2 April 2020. [Online]. Available: https://www.securitymagazine.com/articles/92053-world-economic-forum-releases-guide-on-protecting-from-cyberattacks-during-COVID-19.
14. I. Chomiak-Orsa, A. Rot and B. Blaicke, "Artificial Intelligence in Cybersecurity: The Use of AI Along the Cyber Kill Chain," in *Computational Collective Intelligence*, Cham, Switzerland, Springer, 2019, pp. 406-416.
15. S. A. Petrenko and K. A. Makoveichuk, "Big Data Technologies for Cybersecurity," *CEUR Workshop Proceedings*, vol. 2081, no. 22, pp. 107-111, 2017.
16. M. K. Pratt, "What is SIEM software? How it works and how to choose the right tool," CSO, 28 November 2017. [Online]. Available: https://www.csoonline.com/article/2124604/what-is-siem-software-how-it-works-and-how-to-choose-the-right-tool.html.
17. M. Nanda and B. Parinitha, "Machine Learning and Deep Learning methods for Cybersecurity," *International Research Journal of Engineering and Technology (IRJET)*, vol. 6, no. 4, pp. 2881-2886, 2019.

AUTHORS PROFILE

Alex. R. Mathew , Ph.D. in Computer Science and Engineering (Cyber Security)
Certified Information Systems Security Professional- CISSP - (ISC)2
Microsoft Certified Solutions Expert – MCSE - (Microsoft)
Certified Ethical Hacker – CEH- (EC-Council)
Computer Hacking Forensic Investigator - CHFI- (EC-Council)
Cisco Certified Network Associate (CCNA) – (Cisco)Cisco Certified Network Associate (CCNA R &S) – (Cisco)
IBM Certified Ecommerce Specialist ZAP Certified Web Designer
Security+ (CompTIA)ECSA -EC-Council Certified System Analyst (EC Council)CREST Practitioner Security Analyst- CPSA
Memberships:IEEE, Cisco, EC Council, CompTIA, IBM, Microsoft, CSTA. Alex's areas of expertise include Cyber Security, Ethical Hacking, Cyber Crimes and Digital Forensics Investigation. He is a Certified Information Systems Security Professional and the founder of several cyber security awareness initiatives in India, Asia, Cyprus and Middle East. With over 20 years' experience of consulting and training has developed a large skill set and certification set. He was instrumental initiating and organizing a number of conferences. He has 100+ publications with IEEE, ACM and Scopus Indexed International Journals. Dr.Alex has received a number of awards including the Best Professor, Best Presenter etc. He is a frequently invited speaker and panelist, reviewer at International conferences related to Cyber Security, Technology, Innovation and education. Alex's profile describes a confident and outgoing individual who enjoys the company of other people. He has a persuasive, open style with others, and develops interpersonal relationships quickly and relatively easily. His levels of self-confidence mean that he rarely doubts his abilities in a social situation, although he may find it a little harder to deal with practical or impersonal situations. Alex's communicative and open style means that he tends to be trusting of others, or at least confide information more readily than many other personality types. Because of his social orientation, however, he finds it rather difficult to deal with rejection by other people, thriving as he does on their positive attention. His current research activities are directed towards Cyber Security, Internet of Things (IoT), Security in Next Generation Networks, Smart Technologies, Cybercrimes Investigations.