THE IMPORTANCE OF CYBER THREATS IDENTIFICATION AND COUNTERMEASURES DURING THE COVID-19 PANDEMIC HAVOC IN THE U.S.

Dr. Alain Loukaka and Dr. Shawon Rahman

Abstract **- The current COVID-19 pandemic has impacted the economy worldwide and forced employees to shift to a remote workforce. Work from home also emphasized how organizations must effectively protect against cyber threats. Active or persistent threats have now increased and targeted more home users. The increase in cyber-attacks such as DDoS and Phishing, whereas ransomware shows a slight decline. Malicious users have spread misinformation about COVID-19 awareness, which led to many phishing attacks. Users must understand and recognize social engineering attacks and their respective countermeasures. There is a clear correlation between the rise of online users and the increase in cyberattacks, as expressed in the Routine Activity Theory. Crime will essentially increase because motivated criminals can access probable victims, and security is not relatively present. Cyber vigilance is indispensable and critical during the pandemic. Best security practices are necessary to provide a secure communication environment. No single network effectively promotes full-proof protection against sophisticated cyber attackers. Cybersecurity is yet again the most important factor during these unprecedented times.**

Keywords **- COVID-19; Cyberattack; cybersecurity; Security policy; Social Engineering; Active and Persistent threat; Breach; Hacking; Remote Connection.**

I. INTRODUCTION

The COVID-19 pandemic has forced many organizations Worldwide to re-evaluate their business approach. The pandemic has globally impacted businesses, daily activities, and communications. Many organizations were able to adapt while others faltered. The essential workforce, such as hospitals, nursing homes, police, fire department, grocery stores, and cleaning sanitary services, continued to sustain their respective duties. Many non-essential businesses impacted by the pandemic were not able to sustain and closed temporarily in most cases. Online retailers such as Amazon were able to maintain productivity, whereas their market value drastically increased. Many individuals lost employment and filed for unemployment benefits [1]. Individuals with the ability to shift to work from home (WFH) faced an emerging cyber threat trend. Hackers are now focusing on exploiting remote individuals. Cybercriminals take advantage of the current dire health situation to promote false communication narratives regarding pandemics using social engineering methods. Covid-19 cybersecurity-related threats increase due to the pandemic, and increasing vigilance is vital to mitigate catastrophic events [2]. The Routine Activity Theory (RAT) states that a crime is more likely to occur when motivated offenders, promising targets, and a total absence of security [3] as depicted in figure 1.

Figure 1. Routine Activity Theory Anatomy

II. MATERIALS AND METHODS

The Globally, the COVID-19 pandemic has yield thousands of deaths with millions of confirmed cases [3]. The CDC, Centre for Disease Control, has recommended mask mandate until a suitable vaccine is formulated which biomedical companies such as Pfizer, Moderna, and Johnson & Johnson have invested in. Because more people are working from home and not commuting for work, RAT states that the rate of identifiable suitable targets will increase with online activities, increasing the numbers of potential victims [4]. Users are more likely to increase their digital footprint and more often engage in more social activities such as games, social media, music download, movie streaming, trading, and banking [5]. Because of all the previous behavior factors, it is anticipated that the rate of victimization and online presence will likely increase. Such growth will provide a broader attack surface to malicious users to perform digital crimes. As a result, it can be hypothesized that there will be an increase in (1) Cybercrimes and (2) WFH Utilization Increase activities when data is compared between pre-covid-19 and during the covid-19 pandemic. The United States represented 38% of all threats observed in 2020 [6]. Phishing and DDoS attacks have a respective percentage increase of 19% and 27%, as denoted in the table 1 below.

 ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

Table 1. 2019-20 Covid-19 Attack Trend Data

Cybercrime	2019	2020	% Change
Phishing	224,556	267,372	19.07
Ransomware	46,177,026	14,594,852	-68.39
DDoS	3,800,000	4,830,000	27.11

The encouraging news was that ransomware did have a 68% significant decrease during that very same period, as shown in figure 2 also below:

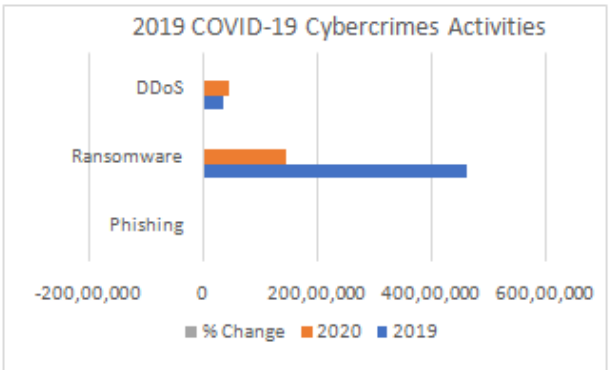

Figure 2. 2019-20 COVID-19 Cybercrimes Increase

Because of the increase in work from home users, stay at home, and school closing, internet service providers (ISP) experienced a massive increase in demand and digital activity during the pandemic [7]. As expected, many users have to utilize business-relatedconferencing applications such as Zoom, WebEx, and Microsoft Meeting to collaborate with their colleagues remotely. Also, children are now learning remotely and utilize the bandwidth. The needed capacity augmentation from ISPs is needed to sustain demand from broadband and cater to home customer users. Also, online social media, gaming, streaming, and shopping increased and are well characterized by Amazon stocks' rise. The digital surge helped cyberthieves spread their misinformation regarding the COVID-19 pandemic, and it was a definite attribute to the rise of phishing and DDoS attacks. Nonetheless, there are many areas of improvement and steps to combat this World crisis [8]. WFH policy must be in place to allow an employee to carry out their daily duties from home. WFH studies do show that employees are more productive from home [9]. It is clear that working from home provides a better sense of comfort and decreases day-to-day stresses from the office. It also helps reduce travel costs and less time commuting. A robust network for communication is vital to combat cyber threats [9]. It is also ideal for organizations to promote VPN use for accessing their infrastructure and cable companies to promote end-to-end security [10]. Cybersecurity is again the most crucial factor. Cybercriminals understand there are fruitful targets to exploits during the pandemic by spreading misinformation [11]. Hackers can always find new sophisticated and straightforward methods to breach a system [12]. Cybersecurity incidents are now increasing at a higher rate due to the current pandemic impact [13]. Users must continue training to identify attacks and how hackers can use the current pandemic to launch attacks based on COVID-19 information [10]. Social engineering must be the core element in every household to combat Phishing, Smishing, and Baiting to avoid lockdown by attackers due to a ransomware virus.

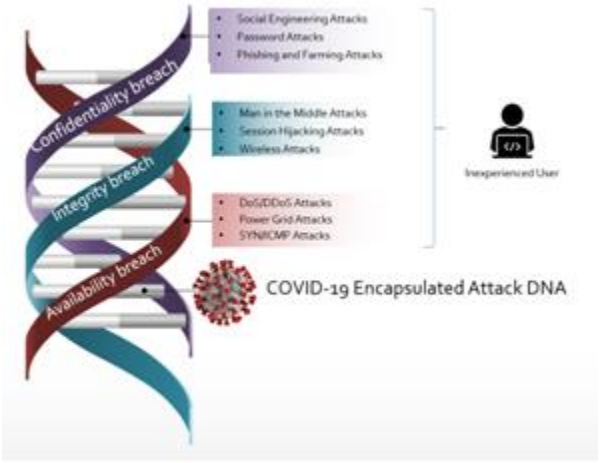

Figure 3. COVIS-19 DNA Attacks

III. RESULTS

The situation is cleared, and cybersecurity is at the forefront in these unpreceded times [10]. Cyber attackers understand the importance of the information flow and understand how vulnerable individuals are regarding security implementation. Users need to understand how to avoid becoming cyber victims. No network is impenetrable, but countermeasures must be in place to thwart any breach. Here are the dire statistics that will increase by 2022 [5] [13]:

- Emails still deliver 94% of malware in 2019 and represent 92% of delivered emails via attachment 48% [14] [15].
- Phishing attacks reached 3,207 emails in 2018 [14].

- Data breaches were 34% and caused by internal threats [15].
- DoS Attacks reached 51% and mainly impacted businesses in 2018 [5].
- Organizations experienced 61% of IoT security incidents [15].
- 90% of Crypto mining was caused by remote code execution attacks [15].
- Mobile devices also have a high application risk download [15].
- Ten thousand five hundred seventy-three average malicious mobile apps were blocked per day in 2018 [14].
- 1 in 13 web requests leads to malware [14].
- Ransomware detections rank highest with 18.2% of all ransomware attacks in the United States [14].

The two hypotheses show a correlation between the rise of cyberattacks due to the rise of online users. The patterns indicate that the increase in cybercrime is due to more online activities. RAT suggests that if there are motivated criminals, more suitable victims, and a lack of security, offenses will occur more frequently. The literature does show the following statistics related to current cybersecurity events during the pandemic [16]:

- 4.66 billion internet users are surfing the net today.
- Internet users grew by 321 million by 2020.
- There were 453 million social users exist between 2019-2020.
- 90% of the Advanced Persistent Threats are comprised of Spear Phishing and cost $2000 to remediate.
- Breaches cost between $8000 and $40000 to organizations.
- 43%, 37%, 27%, and %22 were respectively caused by web application exploit, compromised credentials, Ransomware, and Phishing.

The massive shift in online activity is not necessarily a concern, but the notable increase in cybercrimes is concerning and must be addressed. The distinctive decline of ransomware shows a clear understanding that many organizations and users are significantly less prone to such attacks. However, one-fifth of users fell for social engineer attacks that exposed their data. Denial of service attacks focused more on healthcare government offices and disturbing the flow of information between doctors, hospitals, and clinics. Social distancing and the elevated unemployment rate created an influx of online behavior that contributed to the change of social and economic conditions that increased the victimization rate, as elaborated by RAT [3].

IV. DISCUSSION

Understanding the attack surface and the possibility that a persistent threat can disrupt information technology, users and organizations must be on a continuous high alert since the current pandemic has changed how people work and communicate with each other. The current situation is dire but not impossible to manage beyond a health perspective. Most people are stressed and developed anxiety due to the stay-at-home order and social distancing. Persistent threat actors now understand that the platform for their attacks has increased, and the amplification of devices and applications breaches will more likely increase. Understanding current and possible threats can help promote a continuous security perspective in these difficult economic times for home users. There are countless awareness training and cybersecurity programs organizations must continue to provide remotely. Continuous education for employees is essential to promote identifying some sources of attacks, especially when dealing with social engineering threats. There is a current cybersecurity situation requiring immediate attention at all levels. Besides the gap in the literature regarding information security management, implementing tools and techniques to prevent the exploitation of security flaws is imperative [17]. Here are the standard most type of attacks that will be disturbing social and financial communications during the pandemic with their respective meaning, countermeasures, and mitigation techniques [18]–[22]:

- Fraud/Ransomware/Scareware is meant to steal financial information from the intended target. Fraud can come from a different form and be associated with many more engineering attacks as theft or payment to digital thieves to release stolen information, such as what ransomware is intended to do. Cyber thieves have elaborated schemes to lure future victims into providing their credit card information by promoting or leading from a fraudulent website or hijacking the victim system to hijack it and request payment to release the information to prevent data release publicly or erased. The best scenario is to avoid scams from spammers and avoiding clicking on links from an unknown source. Furthermore, if it is a known source, please very it from the very sender.

- Viruses are common and usually originate from emails. Sometimes, an unaware user is redirected to a fake website that looks like a known site but will send the data to the cyber attacker instead, such as in farming attacks where the attacker collects data. Such

 ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

viruses are also used in a ransomware attack discussed previously to encrypt data where payment is usually requested to release the hijacked data or destroy it. Computer viruses are indeed the most common if proper computer hygiene I not consistently performed. Using antiviruses' software can help with the detection of suspicious activities based on their signatures. Also, rule-based firewalls can prevent traffic from specific I.P. addresses.

- Man The Middle attack (MITM) is also meant to intercept vital communication such as financial data. It is simply a bash where a script allows a cyber attacker to place him/herself between communication and intercept data. It gives the allusion to the user that he/she is communicating with the correct institution or organization. During the attack, the user unknowingly provides the attacker with all the necessary information for them to use and, in most cases, cipher money. Encryption such as Triple DES, Blowfish, and AES (Advanced Encryption Standards) are significant countermeasures to stop the MITM attack by using strong encryption.

- DNS Spoofing is also directly associated with the MITM attack when the attacker is led to the attacker's website and redirects the I.P. traffic to intercept the communication mentioned above.

- Spear/Whaling/Vishing Phishing attacks are, respectively, the art of targeting specific individuals/groups, high profile individuals, and phone calls to get personal information from a person. The attack aims to gain a person's trust, so following up means of attack can ensue, such as an email with a link to a virus and probably gaining access to the network or bringing it down. In such cases, it is essential for anyone receiving a call from an unknown caller pretending to be the person they are not or use authority to be legitimately verified.

• Spreading misinformation on any subject can have adverse results on the population. It does create a platform where confusion and emotional statements contribute to hate and violence. Many groups are using false narratives to promote their agenda y using software such as Facebook and Twitter to spread many false narratives. This attack also relates to MITM, viruses, and DNS spoofing attacks where the user is taken advantage of socially and emotionally to gain their trust so the cyber thieves can take advantage of the situation and extract vital personal and financial data. There is a simple solution to combat this attack is by being open-minded and knowledgeable on the subject. Influence is a great weapon, but knowledge is indeed power.

V. CONCLUSION

The greatest weapon against a threat is understanding the attack surface and implement the necessary countermeasures to fight online attacks. An increasing amount of people become more susceptible to attack because they do not understand or recognize the attack platform and possibility. It is possibly due to confinement fatigue which can allow careless behavior. The tenets of RAT show that crime increased when malicious individuals have more timely access to the victim, and the lack of security presence yields motivated criminals to perform illegal acts. Understandably, people's behavior is changed when their way of life is altered, especially freedom of expression is taken away. Such behavior always leads to susceptible thoughts and exposure to misinformation. This paper does correlate that the increase in online activities comparatively increases cyberattacks. Phishing and DDoS are among the ones that increased significantly because of how people communicate during social distancing. Videoconferencing and online shopping have relatively increased because it is evident that everyone is home shopping more. ISPs have experienced a higher demand in bandwidth to cope with more connectivity nationwide. Hackers adapt to such situations to perform simple to sophisticated attacks, whether physical or virtual. The paramount attitude must be placed on the defensive, meaning understanding what vulnerabilities and threats might be. For instance, never open emails or clickbait when the source is not verified. Such social engineering attacks are still one effective technique to engage the user and install viruses or redirect to a malicious site.

REFERENCES

[1] Brynjolfsson, E., Horton, J. J., Ozimek, A., Rock, D., Sharma, G., & TuYe, H. Y. (2020). Covid-19 and remote work: An early look at U.S. data (No. w27344). National Bureau of Economic Research.

[2] Ramadan, R. A., Aboshosha, B. W., Jalawi, S. A., Alzahrani, A. J., El-Sayed, A., & Dessouky, M. M. (2021). Cybersecurity and countermeasures at the time of pandemic. Journal of Advanced Transportation, 2021 doi:http://dx.doi.org/10.1155/2021/6627264

[3] Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach.American Sociological Review, 44, 588–608.

[4] Maboloc, C. R., Baratipour, M., Parahakaran, S., & D'Astous, M. (2020). Eubios Journal of Asian and International Bioethics.EJAIB,30,3. pp 161-165.

[5] Hawdon, J., Parti, K., & Dearden, T. E. (2020).

 ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

Cybercrime in America amid COVID-19: The initial results from a natural experiment. American Journal of Criminal Justice, 45(4), 546-562.]
[6] World Health Organization. (2020). Coronavirus disease (COVID-19): situation report, 182.
[7] Liu, S., Schmitt, P., Bronzino, F., & Feamster, N. (2020). Characterizing Service Provider Response to the COVID-19 Pandemic in the United States. arXiv preprint arXiv:2011.00419.
[8] Jayakumar, P., Brohi, S. N., & Zaman, N. (2020). Top 7 Lessons Learned from COVID-19 Pandemic.
[9] Dockery, M., & Bawa, S. (2020). Working from Home in the COVID-19 Lockdown. Bentley: Bankwest Curtin Economics Centre.
[10] Ahmad, Tabrez. (2020). Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity. SSRN Electronic Journal. 10.2139/ssrn.3568830.
[11] Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. South African Journal of InformationManagement, 23(1) doi:http://dx.doi.org/10.4102/sajim.v23i1.1277
[12] Loukaka, Alain, & Rahman, Shawon (2020). Security Professionals Must Reinforce Detect Attacks to Avoid Unauthorized Data Exposure. Information Technology in Industry, an International Journal for Research Practitioners, 8(1), 16-30.
[13] Eddy, N. (2020). Cyberattacks continue to mount during the COVID-19 pandemic. Healthcare I.T. News, 8.
[14] Okereafor, K., & Adebola, O. (2020). Tackling the Cybersecurity impacts of the coronavirus outbreak as a challenge to internet safety. Journal Homepage: http://ijmr. net. in, 8(2).
[15] Milanovic, M., & Schmitt, M. N. (2020). Cyber Attacks and Cyber (Mis) information Operations during a Pandemic. Journal of National Security Law & Policy (Forthcoming).
[16] Hejase, H. J., Fayyad-Kazan, H. F., Hejase, A. J., & Moukadem, I. A. (2021). Cyber Security amid COVID-19. Computer and Information Science, 14(2).
[17] Loukaka, Alain, & Rahman, Shawon (2017). Discovering New Cyber Protection Approaches from a Security Professional Prospective. International Journal of Computer Network & Communication (IJCNC), 9(4). Retrieved from ttp://aircconline.com/ijcnc/V9N4/9417 cnc02.pdf
[18] Jartelius, M. (2020). The 2020 Data Breach Investigations Report–a CSO's perspective. Network Security, 2020(7), 9-12.
[19] Symantec, I. (2019). Internet Security Threat Report 2019 [J].
[20] CISCO (2019). Annual Cybersecurity Report. Retrieved from https://www.cisco.com/c/m/en_au/products/security/offers /annual-cybersecurity-report-2018.html
[21] Varshney, S., Munjal, D., Jash, I., Bhattacharya, O., & Saboo, S. (2020). Cyber Crime Awareness and Corresponding Countermeasures. Available at SSRN 3601807. Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. Future Internet, 11(4), 89.

AUTHORS

Dr. Alain Loukaka: Alain Loukaka is a Ph.D. graduate in the Information Security and Information Assurance program at Capella University, Minneapolis, USA. Alain's study was exploratory research on cybersecurity exploits and an advanced method of detection beyond current know application. Alain has a Masters' in Information Technology from Florida Tech and a B.S. in I.T. Networking with a security emphasis from Clayton State College and University. Alain has been in the I.T. field for more than 15 years and plans to use his work to promote better security approaches and deterrents.

Dr. Shawon Rahman: Dr. Shawon S. M. Rahman is a Professor in the Department of Computer Science at the University of Hawaii-Hilo. Dr. Rahman's research interests include Information Assurance and Security, Digital Forensics, Software Engineering Education, Software Testing & Q.A., Cloud Computing, Mobile Application Development, and Web Accessibility. He has published over 125 peer-reviewed articles and is a member of many professional organizations, including IEEE, ACM, ASEE, ASQ, ISACA, ISCA, and UPE.