COVID-19 and Global Increases in Cybersecurity Attacks: Review of Possible Adverse Artificial Intelligence Attacks

1st Aws Naser Jaber
Artificial Intelligence Lab
Oslo Metropolitan University
Oslo, Norway
awsalzar@oslomet.no

2nd Lothar Fritsch
Institute for Information Technology
Oslo Metropolitan University
Oslo, Norway
lotharfr@oslomet.no

***Abstract*—The World Health Organization's (WHO) coronavirus disease dashboard has recorded over 207 million confirmed infections and over 4 million deaths. There has been an increasing vulnerability in cybersecurity amongst businesses, governments and individuals worldwide because the COVID-19 pandemic has led to additional online activities. Accordingly, many people have turned to online work whilst the world is locked down. Thus, warnings have been issued by cybersecurity agencies that the number of cyber threat actors is increasing, and that they are improving in terms of stealing money, personal information and intellectual property. Opportunities for cybercrimes have increased, and COVID-19 is an effective lure. New methods for adverse artificial intelligence (AI)-empowered cyberattacks have been developed, or will be in the near future, using various weaponisations of AI under the COVID-19 umbrella. For this reason, this study reviewed and summarised how and when the most recent cyberattack trends can successfully exploit COVID-19 as a context for attack. Additionally, a summary of the state of knowledge of adverse AI is given, and its potential within the COVID-themed security threats, including defenses, is discussed.**

***Index Terms*—computer security, artificial intelligence, cyberattack, COVID-19**

I. Introduction

Apart from having a collective unprecedented effect on industry and society, the COVID-19 pandemic created a collection of specific circumstances related to cyber crime that have also affected society and business through spam emails [1].]. There has been a spike in crime involving COVID-19, impersonating legitimate businesses, offering suspicious links for receiving money, such as one from MoneyGram or Western Union, or requesting bitcoin payments for face masks [2]. We should be aware of the misleading nature of some emails that claim to be legitimate messages from suppliers. Heightened anxiety induced by the pandemic has raised the likelihood of successful cyberattacks, in which criminals work from all angles, including running phone scams and scheduling fake vaccination appointments [3].

Personal computers at home lack the same security features as those in company networks. This study reviews the COVID-19 pandemic from a cybercrime viewpoint and highlights the number of cyberattacks the pandemic has facilitated internationally. According to the Federal Bureau of Investigation (FBI), there was a large gap between the initial outbreak of the pandemic and the first cyberattack associated with COVID-19, gradually increasing to 4000 attacks daily (FBI) [4]. Ransomware attacks have become prolific as well, increasing 500 times since the start of the pandemic [5].

II. CYBERSECURITY ISSUE DURING THE COVID-19 PANDEMIC

When COVID-19 spread globally, it also resulted in a major secondary challenge to a technology-driven society. A series of cyberattacks and cybercrime initiatives were observed, some indiscriminate and several others targeted [6]. After the outbreak, there have been reports of scams impersonating public officials (e.g. WHO officials) and organisations (e.g. supermarkets and airlines), attacking assistance platforms and offering COVID-19 cures [7]. Such scams target a general audience, as well as the millions of people who work from home (WFH). WFH has presented threats and obstacles to cyber security to a degree that businesses and people have never experienced before.

Cybercriminals have used the aforementioned opportunity to extend their attacks by using common trickery, often preying on the increased tension, fear and insecurity that people experience during the COVID-19 pandemic [8]. However, the shift to WFH has revealed the general level of unpreparedness amongst software sellers, particularly regarding the safety of their products [9]. Cyberattacks have focused on critical infrastructures, such as health services. The US Department of Homeland Security (DHS) released a warning on 8 April 2020 on how cybercriminals exploit the COVID-19 pandemic. [10]. The DHS advisory message covered vulnerability problems, such as phishing, ransomware and infiltration of messaging networks (e.g. Zoom and Microsoft Teams). The following Zoom domains have been targeted by cyber criminals:

© 2022 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

DOI: https://doi.org/10.1109/ICSEC53205.2021.9684603

- www.zoomnow.net
- www.zoomus.top
- www.zoomus.net
- www.zoomus.org
- www.zoomus.cn
- www.zoomcallonline.com (possible malware)
- www.zoomroom.link (possible malware)

Nevertheless, several aspects of society have shifted online with the wide adoption of digital technology, from shopping and social networking to business, industry, and, sadly, even crime. Latest estimates have shown that cybercrime is increasing in frequency and severity, and forecast to cause six trillion dollars in damage by 2021, given that conventional crime has begun to shift online [11].

Cybercrime will continue because of its lucrative nature and low risk level, as cybercriminals can initiate attacks from anywhere globally [12]. Cybercrime, similar to conventional crime, is represented in a criminal triangle, in which three conditions must exist for cybercrime to occur: target, motive and opportunity [13]. Certain criminology models, such as routine activity theory (RAT) [14] and fraud triangle, use similar elements to characterise crimes, with some replacing victims with attackers, who would otherwise be viewed as part of the opportunity [15]. Fig1, shows the RAT triangle.

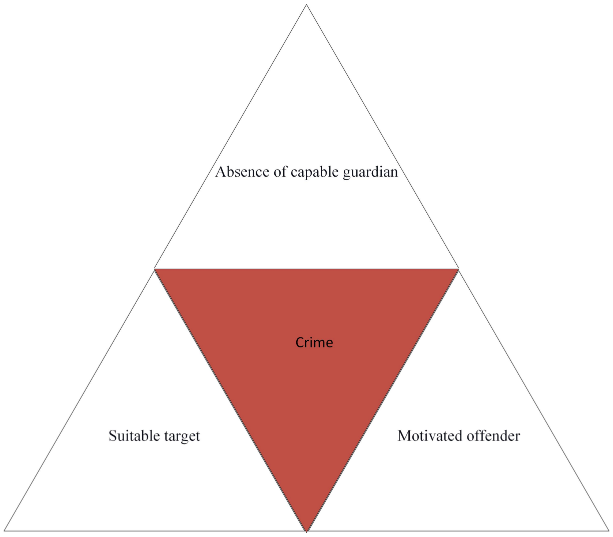


Fig. 1. Fraud Triangle for RAT

Although current attacks have become considerably sophisticated and targeted at victims based on the motive of the attacker, such as financial benefit, spying, coercion or revenge, opportunistic untargeted attacks remain relatively popular [16]. We define 'opportunistic attacks' as attacks that select victims based on their vulnerability to attacks [17]. Opportunistic attackers select victims that have specific vulnerabilities or use hooks, typically in the form of social engineering, to build such vulnerabilities. We define any method used to trick victims into falling prey to attack as a hook. Hooks work by taking advantage of distractions, time constraints, fear and other human factors [18].

Immediately after the beginning of the COVID-19 pandemic, thousands of fake websites appeared calling for humanitarian donations. People received scam emails demanding personal details to obtain future pay-outs or relief effort from the government. Different scams occurred alongside numerous natural disasters, such as the earthquakes in Japan and Ecuador in 2016 2016 [19], Hurricane Harvey in 2017 and bush fires in Australia in 2020 [20]. Notable accidents or events that generated similar scams, include Michael Jackson's tragic death, which dominated globally on 25 June 2009. Spam emails claiming to know the specifics of incidents were circulated online a mere eight hours after his demise [21]. Projections for 2021 are not encouraging, predicting a further increase in security attacks that mostly involve social engineering, sophisticated ransomware and phishing campaigns [22]. Numerous users experienced scams, such as extortion and phishing, and some compromised accounts that had not changed passwords since the breach were used to send phishing links via private message and InMail [23]. Given the number of these scams and cyberattacks, similar attacks that have been perpetrated during the ongoing COVID-19 pandemic are no longer unsurprising.

The pandemic has caused mass disruption globally, with people needing to adjust their everyday lives to a new reality that involves WFH, lack of social and physical activities and fear of not being prepared. Such scenarios may confuse numerous people and cause stress and anxiety, thereby possibly increasing the likelihood of becoming victims of attacks. The abrupt shift in working conditions has also meant that businesses have had to improvise new operating systems, making corporate assets potentially less secure than ever for interoperability. After the beginning of the COVID-19 pandemic, the number of scams and malware attacks has increased significantly [24], with twice the number of phishing attempts from Q4 2020, increasing by 14 percent from Q1 2021 see in Fig2.

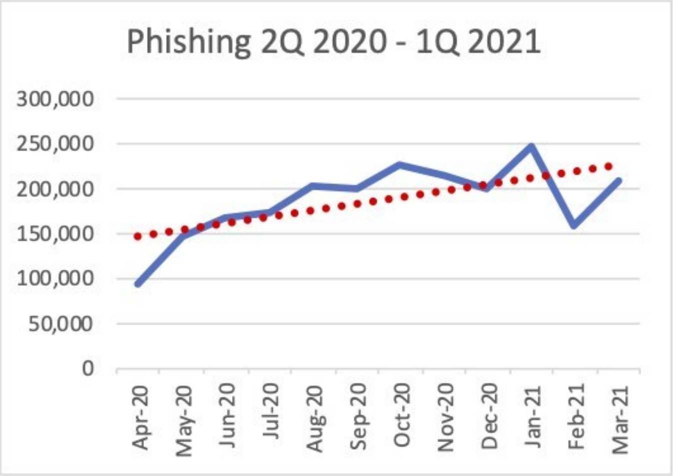


Fig. 2. Phishing attacked increased between Q2 2020 to Q1 2021

Brute force attacks on the networks of the Microsoft Remote Desktop Protocol (RDP) have also increased, signifying that attempts are being made on technology and not just human actors [25]. Evidently, attackers attempt to make the most of the damage caused by the pandemic, particularly given that cyberattacks continue. Consequently,several guidelines and recommendations for defending against attacks have also been published. Such guidelines are crucial in reversing the increasing threat. To strengthen their foundation, a core understanding of cyberattacks being launched firstly need to be identified [26].

III. Current Challenge Of Cybersecurity Attacks

After reviewing and searching cybersecurity attacks from the early COVID-19 to the present, we determined severl types of cybersecurity attacks that have spread widely in this period: spear-phishing and spam emails, malware, website hijacking, website cloning, cyberbullying, and adverse artificial intelligence (AI) attacks in COVID-19 as shown in Fig3. The art of these threats comes from developing a weaponised AI system to automate these attacks. The weaponisation of AI means that attackers may use backdoor poisoning, attacks transfer learning attack, BadNets and threat model gradient-based poisoning.

Properly encrypted secured transmission of medical images need appropriate methods to preserve patient privacy. The objective of this research is to encrypt COVID-19 pictures from the compound tomography (CT) chest to cypher images for the safe transmission of infected patients in the real world. Pseudo-random generators may be used to produce a ‘keystream’ to ensure high-level confidentiality of patient information. The generating Blum Blum Shub (BBS) is a strong generator of pseudo-random bit strings. In [27], the author describes a hack version of BBS, specifically the Hash-BBS (HBBS) generator, which uses a hash function to strengthen the integrity of binary sections removed to create numerous key streams. The NIST trial suite was utilised to evaluate and validate the statistical characteristics of the resulting key bit strings of all the operations performed. The bitstrings obtained exhibited excellent randomisation characteristics, thus a standardised dispersed binary sequence throughout the key length was produced. Based on the key streams acquired, an encryption method, including four COVID-19 CT-images, is suggested and intended to provide considerable anonymity and integrity in medical data transfer. A thorough performance study utilising various assessment measures was also performed.

During the pandemic, password ethics has rapidly increased. In 2020, SpyCloud researchers retrieved over 4.6 billion records of personally identifiable information (PII) and over 1.5 billion stolen login details from 854 data leak sites. According to the company’s 2021 credential exposure analysis, the number of available breach sources increased by 33 percent over 2019, with an average breach size of 5,455,813 records in 2020. Researchers from SpyCloud discovered that 60 percent of passwords were repeated across numerous accounts, enabling hackers to attempt to take over accounts.

A. *Spear-phishing and spam emails*

Numerous scams and phishing attacks are the most prevalent and effective attacks during the pandemic. Phishing attacks have a success rate of over 30 percent [28].It is particularly concerning because attackers just require a low percentage of clicks to generate revenue or accomplish other objectives. Consequently, sending millions of emails to victims pleading for financial assistance from the government, their employers, banks and other sources will result in immediate and large rewards. Numerous phishing attacks (e.g. email, SMS and voice) are launched against vulnerable individuals and systems, with COVID-19 serving as bait [29].

B. *Malware*

Only a few months into the COVID-19 pandemic, fake versions of virus contact tracing apps were observed [30], [31] which contain malware, or attacked banking and finance apps. Liu et al. systematically assess the pandemic’s effects on cybersecurity through malware [32]. Their findings present malware data sets during the COVID-19 pandemic, which include 4,322 coronavirus-themed Android application package APK samples from January 2020 to November 2020. We should considerably focus on apps related to emerging social events [33]. Shifu et al. propose innovative, protective detection techniques based on adversarial generalisation disentanglers to identify anti-Android malware integrated with a COVID-19 app [34]. They successfully integrated their solution with commercialised Dr. HIN products. Aslan and Yilmaz claim that ML and AI is ineffective against new and complex malware developed and used during the pandemic [35]. Therefore, they propose hybrid, optimised and pre-trained network models. Their classification model based on deep learning, AlexNet and Resnet has shown promising results with a 96.5 percent success rate. AI-empowered malware organising its lateral movements with machine learning technology has been observed [36].

C. *Browser hijacking*

Given the COVID-19 pandemic and the necessity of using the Internet for remote work, malicious content on the web has become a global threat to web users. The reason is that its prolific spread has made them vulnerable to all types of electronic attacks that can be implemented behind websites (see Fig4). Al-Ajeej from the research park education continues to pro- pose solutions to detect content that currently refers to COVID-19. However, the use of AI tools in simplified ways has provided considerable opportunity to attackers [36], [37], enabling them to work and develop sophisticated offensive tools, and programming them to use the latest AI methods to delude users into thinking that fake websites are real to hijack sensitive information.

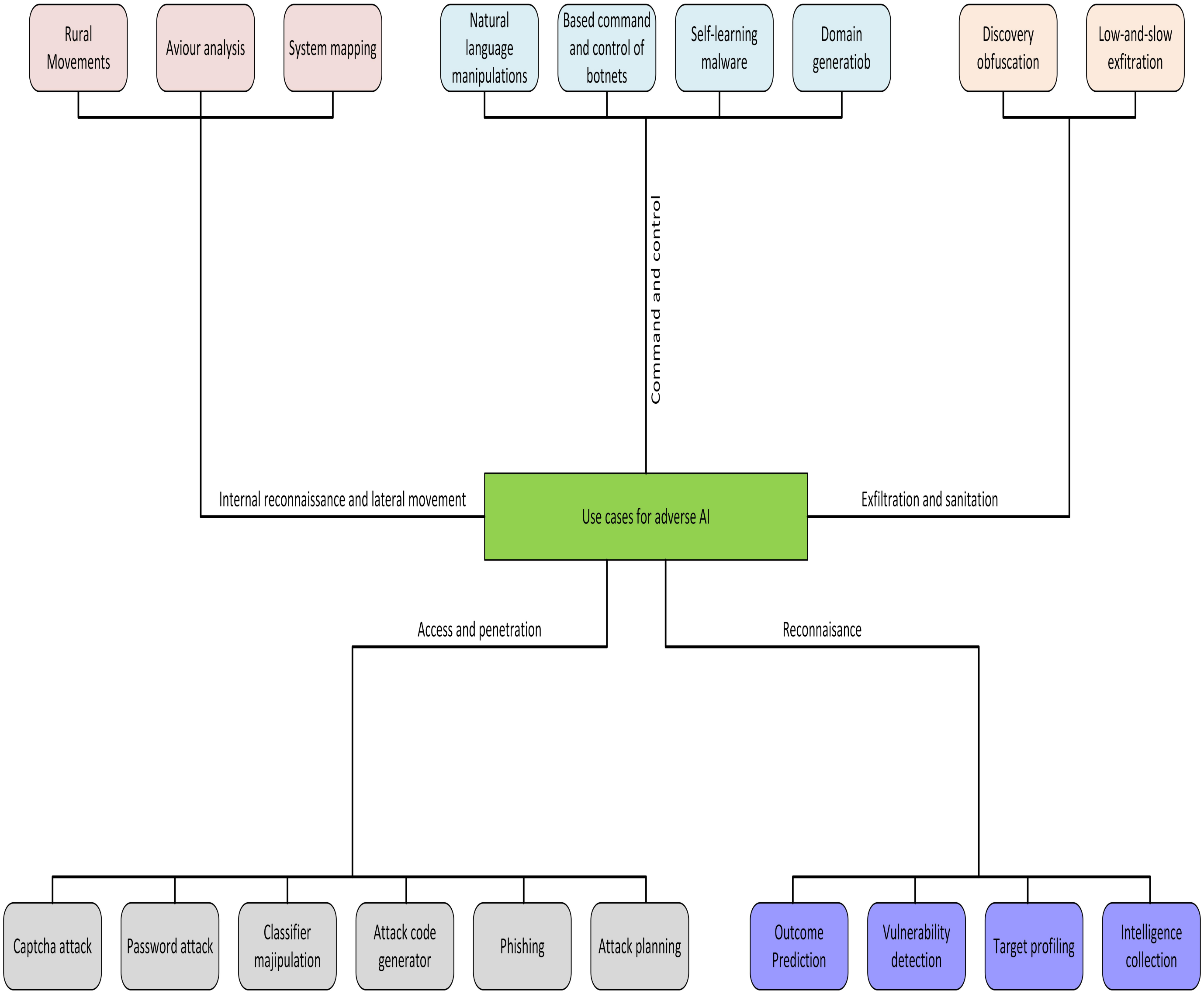


Fig. 3. Adverse AI Attacks in Covid-19

One of the works developed by Khalil recommends a Google Chrome plug-in extension called CovProtectWeb, which detects previously unknown types of COVID-19-related false news [38]. Another related study explored benign and malicious domains using a data set of pandemic-related domains [39]. They used AI tool called Domain Tool. Shannon's entropy was used for the feature extraction, and SVM, k-nearest neighbors (KNN) algorithm and Naive Bayes were used for classification [40]. Their accuracy rate was 99.2% , with a sample size of 7849 domain name [41].

D. *website cloning*

As the pandemic continues, threat actors will attempt to take advantage of individuals globally. Their most recent attempts have included creating fraudulent websites that appear to be connected with COVID-19 financial aid to steal passwords. Numerous credential phishing website templates based on

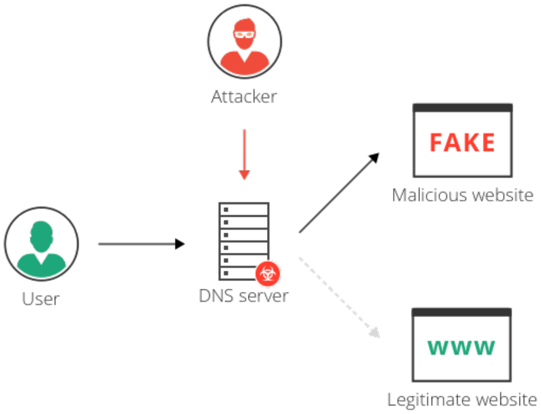
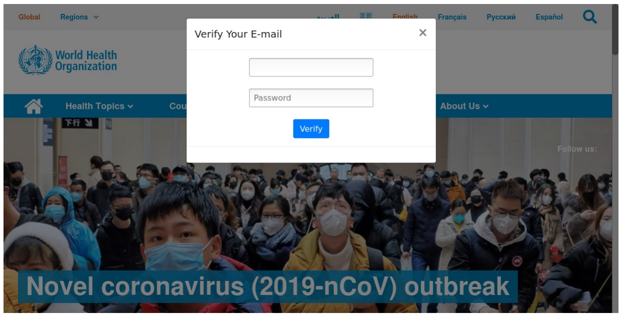


Fig. 4. Phishing attacks

COVID-19 standard have been created, and they mimic the products of multiple governments and trusted non-government organisations (NGOs), including the World Health Organization (WHO), Centers for Disease Control and Prevention (CDC), Internal Revenue Service (IRS) and the governments of Canada, the UK, and France. Phishing-related attacks increased by 530 percent between December 2020 and February 2021, and that phishing-related attacks against drugstores and hospitals increased by 189 percent in the same period. The malicious design intended to steal visitors' login and passwords are shown in in Fig5, purportedly to enable them to obtain information on COVID-19 security protocols. The goal is to steal people's attention. Search engines may be directing visitors to clones, which clone owners may monetise via advertising networks, such as Google Ads, or they may alter clones to mislead readers. However, attackers may duplicate website using several technologies (e.g. HTTrack).



Verify Your E-mail ×

Password

Verify

Fig. 5. WHO Credential Phishing Template Spoofed and cloning

E. Cases for adverse AI-enhanced attacks under the COVID-19 theme

Five categories of AI-enhanced adverse attacks against information security have been identified by the Swedish Defence Research Institute [42]:

1) Reconnaisance: Intelligence collection, target profiling, vulnerability detection, outcome prediction;
2) Access and penetration: Attack planning, phishing and spear phishing, attack code generation, classifier manipulation, password attacks, captcha attacks;
3) Internal reconnaisance and lateral movement: Network and system mapping, network behaviour analysis, smart lateral movements;
4) Command and control: Domain generation, self-learning malware, swarm-based command and control of botnets, natural language manipulations;
5) Exfiltration and sanitation: Slow low-key exfiltration of data, discovery obfuscation;

Concerning their potential for enhancing COVID-19-themed new threats, AI attacks' potential for enhanced phishing attacks, network reconnaisance and password attacks must be stressed. Moreover, their potential to exfiltrate information on network topologies and defence mechanisms in remote work settings. AI-generated or AI-equipped malware camouflaging with health-related COVID-19 themes, including fake contact tracing, which is also a realistic threat to apps [30], [31], [43].

IV. DISCUSSION

Cybercrime events emerging from the COVID-19 pandemic pose significant risks to the world's security and economy, making it important to consider their mechanisms, as well as the scope and reach of those risks. In the literature, various methods have been suggested to examine how these incidents occur, ranging from formal concepts to structural approaches analysing the existence of threats. Even under normal circumstances, cybercrimes, such as fraud, provide the highest earnings with the slightest danger to perpetrators. Given that an increasing number of people become unemployed, they spend considerable time at home and on the Internet for work and socialisation. Additionally, governments and other enterprises have developed incentives to assist individuals financially and attract or retain clients. According to the World Economic Forum's (WEF) study, hacking and phishing have become the new norm, even after the viruses have been eradicated. These frauds are considerably effective currently, during the epidemic, because most susceptible people are fearful and expecting emails, texts, phone calls and other forms of communication from the authorities regarding COVID-19. Given that cybercriminals gain awareness of the situation, it will become much easier for them to create fake messages or websites that appear to be from relevant and familiar authorities, incorporating words that use the word 'urgent' to capitalise on the widely felt fear associated with dealing with an emergency and its requirements. Consequently, fraudsters can improve the effectiveness of their phishing attempts. These forms of attacks include internal and external updates, personal gain and charity. According to a recent F-Secure study, spam is one of the most common means for malware to spread. Additionally, it discussed how attackers are leveraging the epidemic to entice victims to click, most notably by disguising the executable behind archive files such as.zip files. Note that malicious actors may use legitimate information as bait to convince users to take a risky action, such as clicking on a link or opening an attachment. Before acting on an email, users should investigate the sender and any links contained within. Cyber thieves regularly utilise impersonation techniques, such as posing as the WHO, United Nations (UN) or a well-known corporation when they are WFH, Zoom, to trick users into clicking on links or opening infected documents.

Nearly every country has been placed on lockdown as a result of the epidemic. The industry has expressed concerns over the shift to a new working model, in which workers work from home, primarily using employer-secured home systems. As a result of this mass quarantine, new concerns on the resilience of technical solutions in most ecosystems have surfaced, most notably on the resilience of present technology within employers' existing cyberinfrastructures. However, we conclude a mitigating and preventing cyberattacks is a difficult task. Although there are no peer-reviewed publications to date on specific defenses against COVID-19-themed cyberattacks, we can still gain insight from consultancies and commercial vendors on how such attacks can be controlled. We investigated generic advice against such attacks by using the Google search engine with the search terms COVID-19, COVID themed cyberattacks, malware, countermeasure, defense and control. The search results include Internet and software security firms, large software platform vendors, and consulting companies. Most of their blog-published-advice focus on four areas of defense:

1) deployment of up-to-date malware scanners, recommended by nearly all commercial actors;
2) use of anti-phishing tools that sanitize e-mail, filter attack domains and prevent password loss, e.g as recommended by IBM [44] and Microsoft [45];
3) strengthen security culture in organizations, e.g. as recommended by KPMG [46];
4) focus on device mobility, mobile devices and home office situations with blended use of devices, as suggested by McAffee [47].

Apart from this specific advice, attacks that use AI should be observed well, and regular defenses deployed with specific attention to mobile and home working, as descibed in the following sections.

A. Defensive AI against cyberattacks

Researchers have classified cyberattacks in terms of harmful acts performed at various attack stages, but the mechanism that drives them remains unknown. Bayesian reasoning and regression analysis are examples of ML models, as are classifiers (e.g. SVM) and prediction models (e.g. decision trees). ML models include Bayesian reasoning and regression analysis. ML has been combined with other automation approaches, such as neural fuzzing in cybersecurity research for advertise attack findings [48]. According to the National Institute of Standards and Tech- nology, a neural network approach, known as generative adversarial networks (GAN), has recently been connected to deep fakes and false data duplication [49].Two neural networks (i.e. generative and discriminative networks) are used in GAN to replicate content features, analyse those features and improve the realism of how the machine represents those characteristics over time through a training process.

By incorporating AI into the system's development to strengthen security controls, such as vulnerability assessment and scanning, may help improve system robustness. Manual, assisted or completely automated vulnerability assessment are all options. Fully automated vulnerability assessment utilises AI methods, resulting in significant cost savings and time savings. Predictive models for vulnerability categorisation, grouping and rating have been built using ML. Precision, recall and f-score are amongst the assessment measures used to evaluate performance. ML may be used to build risk-analysis models that proactively identify and prioritise security flaws, amongst other things. Automated AI in cybersecurity has also been used to evaluate vulnerabilities, primarily in the field of creating attack plans that can test the security of underlying systems. Automated AI, such as modelling actual adversary sequences of actions or concentrating on harmful threats expressed in the form of attack graphs, is used to simulate attackers' real-time actions. According to [50], if attack plans are produced by an AI system rather than by human specialists, then there is a high chance of discovering additional strategies. Another usage of AI for improving AI in system resilience is code review [51]. Peer code review is a popular best practice in software engineering in which source code is manually evaluated by one or more of the code author's peers (reviewers). Using AI systems to automate the process may save time whilst also allowing for numerous problems to be identified than if they were done manually. For code review assistance, many AI systems are being developed. For example, the Amazon Web Services AI-powered code reviewer from CodeGuru was made publicly accessible since June 2020. Therefore, the use of AI to enhance system resilience has tactical and strategic implications. It reduces the effects of zero-day exploits. Zero-day attacks use vulnerabilities that may be exploited by attackers as long as system providers are unaware of them or there is no patch available to address them. AI lowers the black market value of zero-day attacks by lessening their effect.

Another usage of AI for improving AI in system resilience is code review. Peer code review is a popular best practice in software engineering in which source code is manually evaluated by one or more of the code author's peers (reviewers). Using AI systems to automate the process may save time while also allowing for a larger number of problems to be identified than if they were done manually. For code review assistance, many AI systems are being developed. The Amazon Web Services AI-powered code reviewer from CodeGuru, for example, was made publicly accessible since June 2020. As conclusion,The use of AI to enhance system resilience has both tactical and strategic implications. It does reduce the effect of zero-day exploits. Zero-day attacks make use of vulnerabilities that may be exploited by attackers as long as the system providers are unaware of them or there is no patch available to address them. AI lowers the black market value of zero-day attacks by lessening their effect.

B. User Education

Security is only as strong as its weakest link. Numerous security systems regard humans as the weakest link. Consequently, boosting cybersecurity awareness amongst users through regular training is crucial for minimising risks associated with cyber-attacks on businesses. According to a recent study, only 11 percent of firms provided cybersecurity training to non-cyber security workers in the past year.

C. Virtual Private Network (VPN)

Virtual private network (VPN) is a secure communication channel that encrypts data sent and received between two Internet sites. Utilising a VPN to gain Internet access has become the new standard.

VPN enables enterprises to extend their security requirements to distant personnel by providing two forms of protection: secrecy and integrity.

D. Enable multi-factor authentication

Multi-factor authentication (MFA) makes password guessing and theft more difficult, such as brute force cyber-attacks. Before employees can access companies' internal network from home, they must pro- vide her login and password, as well as a one-time code sent to her cell phone to verify their identity. However, MFA is no longer an option. As more companies implement zero trust security procedures, it has become a norm. Owing to remote and hybrid work settings, which are primarily cloud-based, zero trust and MFA are becoming common. Following the COVID-19 epidemic, there were some signs early in the summer of 2021 that companies may be able to return to a more normal manner of doing things. With the availability of vaccinations, effort is exerted to entice workers back to workplaces. Numerous businesses were unprepared for all that happened. They lacked the necessary infrastructure to accommodate remote workers. There were no security measures, policies or processes in place. IT departments were having difficulty keeping up. Now that more strategies are in place, companies can focus on key objectives and fine-tune their work-from-home processes. Multi-factor authentication, or MFA, is a major component of this.

E. Ensure all network-connected devices have up-to-date anti- malware software

Cybercriminals use a range of malware to prey on the weak. Given that millions of new viruses and strains are developed annually, keeping anti-malware software updated regularly can help reduce the risk of malware-related cyber-attacks.

F. Ensure all network-connected devices have up-to-date anti-malware software

Cybercriminals employ a range of malware to prey on the weak. Since millions of new viruses and strains are developed each year, keeping anti-malware software updated regularly can help reduce the risk of malware-related cyber-attacks.

G. Enable strong company online policy

Organisations have minimal or no time to prepare for WFH situations. A solid and comprehensive WFH policy is necessary to secure data and prevent cyber-attacks. Avoiding essential business conversations in public, using only company-approved video and audio conference lines, amongst others,are instances of effective WFH practices. Policies should also contain a robust and documented recovery strategy,and backup method. Additionally, these plans should be evaluated regularly. The reason is that recent research has indicated that 46 percent of businesses test their recovery and backup methods only once a year or less.

H. Physical security of the home office

protection of home office equipment is crucial. Amongst other tactics, ensure that work computers are not left unattended, use a lock screen or lock the laptop and log off devices after each use.

CONCLUSION

The COVID-19 pandemic has resulted in extraordinary and special social and economic conditions that have been leveraged by cybercriminals. This pandemic and the increased cyberattack rate it triggered have had wider consequences that extend beyond the targets of these attacks. Changes in work habits and socialisation mean that people are now spending more time onlin, and more work from home or mobile environments with flexible arrangements, which opens for attacks. Additionally, unemployment rates have also increased. That is, an increasing number of people may turn to cybercrime to support themselves. Numerous cyberattacks start with a COVID-19-themed phishing campaign directing victims to download a file or to access a URL to install malware or to harvest access credentials. Mobile malware camouflaged as COVID-apps is widely observed. Attacks are increasingly using AI and machine learning to generate better phishing messages, better phishing servers and less detectable malware. Although there are some current studies on countermeasures, current controls for COVID-19-themed attacks address classic elements of cybersecurity: anti-phishing systems, malware scanners, a security culture in organisations that covers rules for mobile and home office working situations and a special focus on mobile devices and mixed private/organisational platforms. To date, the use of AI against adversaries has been limited to the techniques used in malware detection, network security and phishing prevention that pre-existed the COVID- 19 pandemic. Hence, opportunities for improving cybersecurity exist. In future research, specific weaponised AI cyber kill chain frameworks for specific sectors and specific attack themes will be produced.

ACKNOWLEDGMENT

The authors thank the OsloMet Artificial Intelligence Lab (Norway) for full financial support.

REFERENCES

[1] Harjinder Singh Lallie, Lynsay A Shepherd, Jason RC Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens. Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *arXiv preprint arXiv:2006.11929*, 2020.

[2] Mohamed Chawki. *Cybercrime in the Context of COVID-19*, pages 986–1002. Springer, 2021.

[3] Harjinder Singh Lallie, Lynsay A Shepherd, Jason RC Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens. Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *arXiv preprint arXiv:2006.11929*, 2020.

[4] Zaina ALsaed and Mahmoud Jazzar. Covid-19 age: Challenges in cybersecurity and possible solution domains. *Journal of Theoretical and Applied Information Technology*, 99(11), 2021.

[5] Harun Oz, Ahmet Aris, Albert Levi, and A Selcuk Uluagac. A survey on ransomware: Evolution, taxonomy, and defense solutions. *arXiv preprint arXiv:2102.06249*, 2021.

[6] Tim Ken Mackey, Jiawei Li, Vidya Purushothaman, Matthew Nali, Neal Shah, Cortni Bardier, Mingxiang Cai, and Bryan Liang. Big data, natural language processing, and deep learning to detect and characterize illicit covid-19 product sales: Infoveillance study on twitter and instagram. *JMIR public health and surveillance*, 6(3):e20794, 2020.

[7] Ruti Gafni and Tal Pavel. Cyberattacks against the health-care sectors during the covid-19 pandemic. *Information & Computer Security*, 2021.

[8] Rennie Naidoo. A multi-level influence model of covid-19 themed cybercrime. *European Journal of Information Systems*, 29(3):306–321, 2020.

[9] Deborah R Farringer. Maybe if we turn it off and then turn it back on again? exploring health care reform as a means to curb cyber attacks. *Journal of Law, Medicine & Ethics*, 47(S4):91–102, 2019.

[10] Gary Ackerman and Hayley Peterson. Terrorism and covid-19. *Perspectives on Terrorism*, 14(3):59–73, 2020.

[11] Moutushi Singh and Indraneel Mukhopadhyay. Cyber security issues in the covid-19 times. In *Proceedings of International Conference on Computational Intelligence, Data Science and Cloud Computing*, pages 671–680. Springer, 2021.

[12] Jip Laan. *The impact of the Corona-pandemic on the business model of cybercrime*. PhD thesis, University of Twente, 2021.

[13] Jacqueline M Drew. A study of cybercrime victimisation and prevention: exploring the use of online crime prevention behaviours and strategies. *Journal of Criminological Research, Policy and Practice*, 2020.

[14] Asif Shaikh and Diogo Oliveira. Informal it and routine activity theory-a theoretical review. In *2019 SoutheastCon*, pages 1–4. IEEE, 2019.

[15] Shaio Yan Huang, Chi-Chen Lin, An-An Chiu, and David C Yen. Fraud detection using fraud triangle risk factors. *Information Systems Frontiers*, 19(6):1343–1356, 2017.

[16] Hasan Awni Shakir and Aws Naser Jaber. A short review for ransomware: pros and cons. In *international conference on P2P, parallel, grid, cloud and internet computing*, pages 401–411. Springer, 2017.

[17] Gurdip Kaur, Ziba Habibi Lashkari, and Arash Habibi Lashkari. *Introduction to Cybersecurity*, pages 17–34. Springer, 2021.

[18] Diana Tietjens Meyers. *Victims' stories and the advancement of human rights*. Oxford University Press, 2016.

[19] Pablo R Izurieta Andrade. *Boom and Bust: Ecuador's Financial Rollercoaster: The interplay between finance, politics and social conditions in 20th Century Ecuador*. Vernon Press, 2017.

[20] Francisco Moreira, Davide Ascoli, Hugh Safford, Mark A Adams, José M Moreno, José MC Pereira, Filipe X Catry, Juan Armesto, William Bond, and Mauro E González. Wildfire management in mediterranean-type regions: paradigm change needed. *Environmental Research Letters*, 15(1):011001, 2020.

[21] Trevor J Blank. *Folklore and the Internet: Vernacular expression in a digital world*. University Press of Colorado, 2009.

[22] Ronny Richardson, Max M North, and David Garofalo. Ransomware: The landscape is shifting–a concise report. *International Management Review*, 17(1):5–86, 2021.

[23] Abdul Basit, Maham Zafar, Xuan Liu, Abdul Rehman Javed, Zunera Jalil, and Kashif Kifayat. A comprehensive survey of ai-enabled phishing attacks detection techniques. *Telecommunication Systems*, 76(1):139–154, 2021.

[24] Pengcheng Xia, Haoyu Wang, Xiapu Luo, Lei Wu, Yajin Zhou, Guangdong Bai, Guoai Xu, Gang Huang, and Xuanzhe Liu. Don't fish in troubled waters! characterizing coronavirus-themed cryptocurrency scams. *arXiv preprint arXiv:2007.13639*, 2020.

[25] APWG Q1 2021 Report. Detected phishing websites maintain historic high in q1 2021, after doubling in 2020'. *APWG*, 2021.

[26] Tim Bai, Haibo Bian, Abbas Abou Daya, Mohammad A Salahuddin, Noura Limam, and Raouf Boutaba. A machine learning approach for rdp-based lateral movement detection. In *2019 IEEE 44th Conference on Local Computer Networks (LCN)*, pages 242–245. IEEE, 2019.

[27] Omar Reyad and Mohamed Esmail Karar. Secure ct-image encryption for covid-19 infections using hbbs-based multiple key-streams. *Arabian Journal for Science and Engineering*, 46(4):3581–3593, 2021.

[28] Max Clasen, Fudong Li, and David Williams. Friend or foe: An investigation into recipient identification of sms-based phishing. In *International Symposium on Human Aspects of Information Security and Assurance*, pages 148–163. Springer, 2021.

[29] Alejandro Correa Bahnsen, Ivan Torroledo, Luis David Camacho, and Sergio Villegas. Deepphish: simulating malicious ai. In *2018 APWG symposium on electronic crime research (eCrime)*, pages 1–8, 2018.

[30] Singcert warns of fake covid-19 contact tracing apps containing malware. https://www.channelnewsasia.com/singapore/covid-19-singcert-fake-contact-tracing-apps-download-privacy-725536, 2020.

[31] Alex Scroxton. Fake contact-tracing apps delivering banking trojans. https://www.computerweekly.com/news/252484584/Fake-contact-tracing-apps-delivering-banking-trojans, 2020.

[32] Liu Wang, Ren He, Haoyu Wang, Pengcheng Xia, Yuanchun Li, Lei Wu, Yajin Zhou, Xiapu Luo, Yulei Sui, Yao Guo, et al. Beyond the virus: A first look at coronavirus-themed mobile malware. *arXiv preprint arXiv:2005.14619*, 2020.

[33] Sunil Kumar Muttoo and Shikha Badhani. An analysis of malware detection and control through covid-19 pandemic. In *2021 8th International Conference on Computing for Sustainable Global Development (INDIACom)*, pages 637–641. IEEE, 2021.

[34] Shifu Hou, Yujie Fan, Mingxuan Ju, Yanfang Ye, Wenqiang Wan, Kui Wang, Yinming Mei, Qi Xiong, and Fudong Shao. Disentangled representation learning in heterogeneous information network for large-scale android malware detection in the covid-19 era and beyond. In *35th AAAI Conference on Artificial Intelligence (AAAI)*, 2021.

[35] Ömer Aslan and Abdullah Asim YILMAZ. A new malware classification framework based on deep learning algorithms. *IEEE Access*, 2021.

[36] Nektaria Kaloudi and Jingyue Li. The ai-based cyber threat landscape: A survey. *ACM Computing Surveys (CSUR)*, 53(1):1–34, 2020.

[37] M Caldwell, JTA Andrews, T Tanay, and LD Griffin. Ai-enabled future crime. *Crime Science*, 9(1):1–13, 2020.

[38] Belouadh et al. *Web Browser Extension for Detecting Covid-19 Themed Malicious Web Content*. PhD thesis, Faculty: Mathimatics and Computer Science Departement: Computer Science, 2021.

[39] Shahid Anwar, Jasni Muhamad Zain, Mohamad Fadli Zolkipli, Zakira Inayat, Aws Naser Jabir, and Julius Beneoluchi Odili. Response option for attacks detected by intrusion detection system. In *2015 4th International Conference on Software Engineering and Computer Systems (ICSECS)*, pages 195–200. IEEE, 2015.

[40] Shahid Anwar, Jasni Mohamad Zain, Zakira Inayat, Riaz Ul Haq, Ahmad Karim, and Aws Naser Jabir. A static approach towards mobile botnet detection. In *2016 3rd International Conference on Electronic Design (ICED)*, pages 563–567. IEEE, 2016.

[41] Jamil Ispahany and Rafiqul Islam. Detecting malicious covid-19 urls using machine learning techniques. In *2021 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*, pages 718–723. IEEE, 2021.

[42] Erik Zouave, T Gustafsson, M Bruce, and K Colde. Artificially intelligent cyberattacks. Technical Report FOI-R-4947-SE, Swedish Defense Research Intsitute (FOI), 2020.

[43] Lars Baumgärtner, Alexandra Dmitrienko, Bernd Freisleben, Alexander Gruler, Jonas Höchst, Joshua Kühlberg, Mira Mezini, Richard Mitev, Markus Miettinen, Anel Muhamedagic, Thien Duc Nguyen, Alvar Penning, Dermot Pustelnik, Filipp Roos, Ahmad-Reza Sadeghi, Michael Schwarz, and Christian Uhl. Mind the gap: Security and privacy risks of contact tracing apps. In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pages 458–467, 2020.

[44] Wendy Withmore and Gary Parham. The covid-19 cyberwar: How to protect your business. https://www.ibm.com/thought-leadership/institute-business-value/report/covid-19-cyberwar (accessed 31-08-2021), 2020.

[45] Tanmay Ganacharya. Protecting against coronavirus themed phishing attacks. https://www.microsoft.com/security/blog/2020/03/20/protecting-against-coronavirus-themed-phishing-attacks/ (accessed 31-08-2021), 2020.

[46] Aknhilesh Tuteja and David Ferbrache. Identifying and responding to covid-19 themed cyber threats. https://home.kpmg/xx/en/home/insights/2020/03/covid-19-staying-cyber-secure.html (accessed 31-08-2021), 2021.

[47] Divya Kala Bhavani. Beware coronavirus-themed cyber-attacks, urges mcafee. The Hindu online, https://www.thehindu.com/sci-tech/technology/internet/mcafee-2021-consumer-mindset-report-covid19-cybersecurity-internet-habits-india/article34699465.ece (accessed 31-08-2021), 2021.

[48] Yan Wang, Peng Jia, Luping Liu, Cheng Huang, and Zhonglin Liu. A systematic review of fuzzing based on machine learning techniques. *PloS one*, 15(8):e0237749, 2020.

[49] Wengang Ma, Yadong Zhang, Jin Guo, and Kehong Li. Abnormal traffic detection based on generative adversarial network and feature optimization selection. *International Journal of Computational Intelligence Systems*, 14(1):1170–1188, 2021.

[50] Saad Khan and Simon Parkinson. Discovering and utilising expert knowledge from security event logs. *Journal of Information Security and Applications*, 48:102375, 2019.