Characterizing the Landscape of COVID-19 Themed Cyberattacks and Defenses

Mir Mehedi Ahsan Pritom*, Kristin M. Schweitzer†, Raymond M. Bateman†, Min Xu‡ and Shouhuai Xu*

*Department of Computer Science, University of Texas at San Antonio
†U.S. Army Research Laboratory South - Cyber
‡Mastercard

Abstract—**COVID-19 (Coronavirus) hit the global society and economy with a big surprise. In particular, work-from-home has become a new norm for employees. Despite the fact that COVID-19 can equally attack innocent people and cyber criminals, it is ironic to see surges in cyberattacks leveraging COVID-19 as a theme, dubbed *COVID-19 themed cyberattacks* or *COVID-19 attacks* for short, which represent a new phenomenon that has yet to be systematically understood. In this paper, we make a first step towards fully characterizing the landscape of these attacks, including their sophistication via the Cyber Kill Chain model. We also explore the solution space of defenses against these attacks.**

Index Terms—**COVID-19 Cyberattacks, Malicious Websites, Malicious Emails, Malicious Mobil Apps, Malicious Messaging, Misinformation, Cyber Kill Chain, Defense**

I. Introduction

The COVID-19 (Cronavirus) pandemic has had a huge impact on the global society and economy. It attacks everyone, including both the innocent people and the cyber criminals. Ironically, we have witnessed surges in cyberattacks leveraging COVID-19 as a theme, dubbed *COVID-19 themed cyberattacks* or *COVID-19 attacks* for short. For example, there is a 32x increase in the malware and phishing sites from February 25, 2020 to March 25, 2020 [1]; Google has been blocking 240 million COVID-19 related spam emails and 18 million phishing and malware emails daily [2]; there is a 148% increase in ransomware attacks in March 2020 over February 2020 [3]. The situation is further exacerbated by the new norm of work-from-home because employees' home computers or devices are often less protected than their enterprise counterparts. Indeed, a CheckPoint survey [4] shows that 55% of security professionals are concerned with remote access and 47% are concerned with their employees using shadow IT systems from their home. Until now, COVID-19 attacks have mainly targeted the finance, healthcare, government, media streaming, retail business, and COVID-19 research sectors. In response, experts have recommended using multi-factor authentication for critical transactions, virtual private networks for remote access, and regularly patching and updating software as immediate solutions [5]. However, given that COVID-19 attacks are a new phenomenon that is here to stay, it is important to understand them thoroughly to pave a way for effective defense.

Our contributions. In this paper, we make a first step towards understanding COVID-19 themed cyberattacks. Specifically, we explore five classes of them, namely malicious websites, malicious emails, malicious mobile apps, malicious messaging, and misinformation. In order to characterize these attacks, we map them to the Cyber Kill Chain model [6]. We show that they can use multiple attack techniques to achieve multiple attack goals. We find that COVID-19 attackers have been professional rather than opportunistic and have been heavily employing social-engineering cyberattacks. We further explore the solution space of defenses against COVID-19 attacks. Since COVID-19 attacks do have their counterparts that are not specific to the COVID-19 incidents, our focus is on exploring the COVID-19 specific aspects. To the best of our knowledge, this is the first systematic characterization of COVID-19 attacks and defenses, which can be adapted to cope with any "X-themed cyberattacks" that may emerge in the future, where X can be any kind of social incidents (e.g., election, natural or man-made disaster).

Related work. The problem of COVID-19 attacks has started to receive attention from the research community. There are studies on the types of cyberattacks and their trends amid the COVID-19 pandemic [7]–[9], studies on specific cyberattacks related to COVID-19 (e.g., mobile malware ecosystem [10], [11], cybercrimes [12], fake news related to COVID-19 [13], and COVID-19 themed cryptocurrency scams [14]). When compared with these studies, we aim at systematically characterizing the landscape of the COVID-19 attacks, including their sophistication through the the Kill Chain [6] and exploring the space of defenses against these attacks.

Paper outline. Section II characterizes COVID-19 attacks. Section III explores the defense solution space. Section IV concludes the paper.

II. Characterizing COVID-19 Attacks

We characterize 5 classes of COVID-19 attacks: malicious websites, malicious emails, malicious mobile apps, malicious messaging, and misinformation. For this purpose, we collect existing news reports and blogs on relevant cyberattacks, manually verify them, and propose mapping them to the Lockheed Martin's Cyber Kill Chain [6], which is a model consisting of the following 7 stages. (i) *Reconnaissance*, which corresponds to pre-attack plannings, finding vulnerabilities, collecting possible victims, and setting attack goals. (ii) *Weaponization*, which corresponds to setting up attack propagation mediums, injecting malicious contents into the mediums, and setting

up traps to fool the identified victims. (iii) *Delivery*, which corresponds to the attacker's penetration into a victim's system through some entry point. (iv) *Exploitation*, which corresponds to the wage of actual attacks against a victim's system. (v) *Installation*, which corresponds to the installation of malicious payloads on a victim's system. (vi) *Command-and-Control* (C2), which corresponds to the attacker's use of remote access to the victims' systems. (vii) *Objectives*, which corresponds to the accomplishment of the attacker's pre-determined goal.

A. COVID-19 Themed Malicious Websites

Attackers have abused websites to wage COVID-19 attacks to steal login credentials, sell fake medications related to COVID-19, and inject malicious payloads into these themed websites to distribute malware [7], [8], [15]. We map these attacks to the Cyber Kill Chain model as follows.

(i) *Reconnaissance:* An attacker selects target audience, chooses a COVID-19 related target theme, searches for cheap and unregulated domain registration and web hosting services, and sets attack goals. (ii) *Weaponization:* An attacker registers new websites with COVID-19 related names. For example, an attacker may register websites with typo-squatting names to mimic legitimate websites related to COVID-19 (e.g., CDC, WHO, FDA) [16]; an attacker may register websites to imitate legit Virtual Private Network (VPN) software or remote communication software; an attacker may register domains to offer fake legal services related to COVID-19; an attacker may change an existing phishing website to accommodate COVID-19 themes; an attacker may register fake media streaming domains; and an attacker may register fake donation websites. (iii) *Delivery:* An attacker hosts COVID-19 themed malicious websites mentioned above. (iv) *Exploitation:* Victims visit malicious websites, and then trust the fake forms or download malicious payloads to their devices. (v) *Installation:* A victim may provide sensitive information to a malicious website or intentionally/unintentionally install malware. (vi) *C2:* An attacker remotely controls victims' infected computers, for example instructing its agents (e.g., malicious websites, downloaded malware) to send the stolen data/credentials to the attacker. (vii) *Objectives:* An attacker gets sensitive credentials, encrypts a victim's computer, or gets ransom payment.

B. COVID-19 Themed Malicious Emails

Attackers have abused emails to wage COVID-19 attacks to send phishing, spamming, scamming, malicious attachments, and malicious websites [17]. We map these attacks to the Cyber Kill Chain model as follows.

(i) *Reconnaissance:* An attacker selects target audience, generates and profiles email lists, selects a target topic for COVID-19 themed lures, and sets an attack goal. (ii) *Weaponization:* An attacker creates fake typo-squatting email addresses imitating legitimate entities (e.g., CEO, Netflix support team, medical doctors), writes malicious emails with legitimate logo (e.g., WHO, hospital logo) and authority names, writes emails with COVID-19 related information and offers, writes emails with malicious attachments [18], [19],

writes fake COVID-19 donation scam emails [20], writes emails with fake financial relief payments [15], writes emails with blackmailing schemes (e.g., threatening languages) [21], writes emails to lure victims to provide personal information or pay fees for false unemployment training and certification [22]. (iii) *Delivery:* An attacker sends the aforementioned emails to the target audience. (iv) *Exploitation:* A victim trusts an email received from an attacker, clicks its malicious links, opens its attachments, or downloads its malicious contents. (v) *Installation:* A victim replies to the attacker with sensitive personal information or installs malicious content on its computer either intentionally or unintentionally. (vi) *C2:* An attacker establishes connections with victim's devices through C2 channels, for example, to instruct the compromised computers to send back sensitive data. (vii) *Objectives:* An attacker encrypts a victim's computer, receives ransom payment, or receives sensitive information.

C. COVID-19 Themed Malicious Mobile Apps

Attackers have abused mobile apps to wage COVID-19 attacks to distribute malware and steal information from the victims [10]. Google and Apple have taken steps during this pandemic to reject publishing of COVID-19 related mobile apps from unauthorized entities [23]. Despite these efforts to secure reputed app stores, malicious apps could still get published and remain undetected as many third party app stores do not have proper reviewing and regulation for publishing apps. Reports showing third-party app stores are eight times more likely to contain malicious apps than than Google Play store [24]. We map the attack of COVID-19 themed malicious mobile apps to the Cyber Kill Chain model as follows.

(i) *Reconnaissance:* An attacker selects target audience (e.g., based on geographical region), selects a COVID-19 themed topic/service (e.g., tracing, tracking, maps, VPN, remote meeting, COVID-19 guidelines, COVID-19 test information), finds and selects profitable unregulated app stores, and sets attack goals. (ii) *Weaponization:* An attacker creates fake mobile apps with typo-squatted app names and legitimate logos to imitate authentic apps, repackages existing COVID-19 themed legitimate apps with malware or ransomware (e.g., banking Trojan, spyware) to trick users [10]. (iii) *Delivery:* An attacker uploads malicious apps into the unregulated app stores or code repositories, and advertises these mobile apps through websites pop-ups. (iv) *Exploitation:* A victim trusts an malicious app and downloads the app. (v) *Installation:* A victim installs the downloaded malicious app on an mobile device. (vi) *C2:* An attacker remotely controls victims' compromised mobile devices to send sensitive user data to the C2 server. (vii) *Objectives:* An attacker encrypts a victim's mobile device, gets a ransom payment, or steals a victim's private information (e.g., login credentials, crypto wallet passwords), breaches user privacy (e.g., location).

D. COVID-19 Themed Malicious Messaging

Attackers have abused messaging services to wage COVID-19 attacks (e.g., phishing, malware, spamming, and scamming)

[9]. COVID-19 has increased the usage of mobile devices which create more incentives for attackers. These attacks are similar to malicious email attacks, but are unique in that messaging can offer more emotional and persuasive live chats. We map them to the Cyber Kill Chain model as follows.

(i) *Reconnaissance:* An attacker selects target audience (e.g., based on demography, geography, severity of COVID-19 infections), collects phone and social media contacts, selects target platform (e.g., Facebook, WhatsApp, Twitter), chooses a COVID-19 themed topic (e.g., fake cures, products, services), and sets attack goals. (ii) *Weaponization:* An attacker writes persuasive and emotional messages (e.g., asking for COVID-19 donations) to trick victims, creates fake social media profiles, and creates social media groups to lure target audience. (iii) *Delivery:* An attacker sends malicious messages, website links, and attachments through messaging to targeted victims, sends scams mentioning fines for leaving home during stay-at-home orders [9], sends fraud messages with free subscription lures for media streaming services [7], sends messages to sell low-quality supplies (e.g., masks, gloves, fake cures, and illegal chemical materials) [25], sends COVID-19 related lucrative offers (e.g., giveaways, loans, lawyer help, food stamps, stimulus check updates, news guidelines), and sends crafted misinformation messages with fake claims and made up evidence. (iv) *Exploitation:* A victim trusts a received message and falls victim to it by clicking its malicious links, downloading its malicious contents, and forwarding it to other users. (v) *Installation:* A victim intentionally or unintentionally installs the malicious payload on an messaging device (e.g. Android mobile phone). (vi) *C2:* An attacker establishes channels (e.g., reply messages, servers connected to a phishing webpage) to remotely control the compromised messaging devices, for example, to receive victims' sensitive information. (vii) *Objectives:* An attacker gets victims' sensitive information or makes lateral movements in victims' networks.

E. COVID-19 Themed Misinformation

Attackers have waged COVID-19 attacks to spread misinformation, which includes false or inaccurate information (e.g., hoaxes, rumors, or propaganda [26]). Examples include: "COVID-19 is invented in a Chinese lab [27]"; "5G is spreading COVID-19 [28]", "Black are immune to COVID-19 [29]", "X can cure COVID-19" where X can be a drug or food items (i.e., Ginger) [30], or "Wearing a mask causes you to inhale too much carbon dioxide, which can make you sick" or "Wearing a mask can result in getting pneumonia" [31]. Social media and messaging platforms further increase the impact of such misinformation. The term *Infodemic* has even been coined because of this [32]. We map the COVID-19 themed misinformation attack to the Cyber Kill Chain as follows.

(i) *Reconnaissance:* An attacker analyzes the characteristics of targeted audience (e.g., ethnicity, demography or nationality), identifies vulnerable divisions in society, selects themed topics, and sets attack goals. (ii) *Weaponization:* An attacker writes fake COVID-19 themed statements and mix them with false evidence and out-of-context truths, creates fake groups

in social networking platforms, creates themed memes, creates bots in social media (e.g., Twitter) to propagate misinformation, and infiltrates into social media groups containing targeted ethnic audience. (iii) *Delivery:* An attacker posts and shares COVID-19 related misinformation (e.g., narratives, memes, images, and hashtags through social media groups and messaging apps) and publishes fake news on paid online news/tabloids, and/or keeps posting to a larger audience with bots to amplify the impact. (iv) *Exploitation:* A victims (e.g., social media user) reads and forwards misinformation messages. (v) *Installation:* A victims gets to believe the misinformation which goes viral. (vi) *C2:* An attacker may generate fake real-life incidents/experience posts on social media related to COVID-19. (vii) *Objectives:* An attacker succeeds when bringing more division, mistrust, health crisis, and chaos in society, and possibly earns money from the crisis.

F. Systematizing COVID-19 Themed Cyberattacks

We systematize COVID-19 attacks by mapping them to their attack techniques and attack goals, and by contrasting their Cyber Kill Chain models.

1) Mapping Attacks, Techniques and Goals: Figure 1 depicts the mapping between the COVID-19 attacks, the attack techniques they use, and their attack goals. We observe that one attack may use multiple attack techniques. For example, a COVID-19 themed malicious website attack may use a range of attack techniques, including phishing, malware, ransomware, vaccine scams, donation scams, masks scams, testing scams, and VPN scams. Moreover, a COVID-19 themed malicious website attack may have multiple goals. On the other hand, one goal can be achieved by using various kinds of attack techniques, which may be waged through multiple classes of attacks. This means that when an attacker attempt to achieve an attack goal, the attacker can choose attacks and attack techniques in a cost-effective, if not optimal, fashion. For example, each attack may incur some cost or risk (e.g., the cost for using phishing via COVID-19 themed malicious websites and COVID-19 themed malicious emails may be different), and may have different success probabilities (e.g., phishing via COVID-19 themed malicious websites may be more or less successful than phishing via COVID-19 themed malicious emails). This would allow an intelligent attacker to wage the cost-effective or event optimal attack. A systematic framework for achieving this type of attacker decision-making is beyond the scope of the present paper.

Insight 1: A COVID-19 attack may use multiple attack techniques to achieve multiple attack goals, and an attack goal may be achieved by using multiple attack techniques that can correspond to multiple attacks. This flexibility allows the attacker to choose cost-effective, if not optimal, attacks in order to achieve a certain attack goal.

2) Systematizing Attacks via Their Cyber Kill Chains: Figure 2 depicts the Cyber Kill Chain mappings of the aforementioned 5 classes of COVID-19 attacks, which are represented by different colors. We observe that in each stage of the Cyber Kill Chain, there can be multiple *tactics* (e.g.,
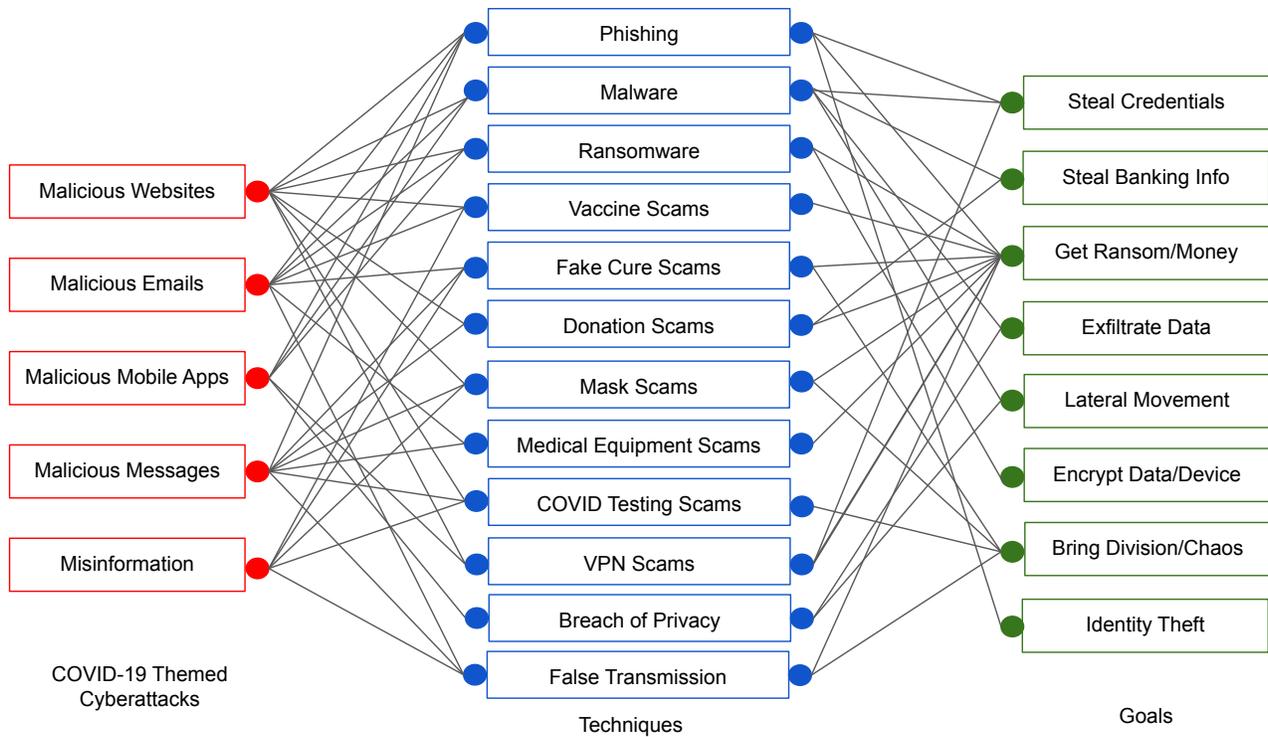
Fig. 1. Systematizing COVID-19 attacks (red), attack techniques (blue), and attack goals (green)

Fig. 2. Systematizing the Cyber Kill Chains for COVID-19 themed cyberattacks, which are coded in colors (see Legend).

"select target audience" and "choose COVID-19 theme topic" at the reconnaissance stage). We observe that the 5 classes of COVID-19 attacks would use some common tactics at some stages as well as their distinct tactics at other stages. For example, "select target audience" at the reconnaissance stage is a tactic that can be used by the 5 classes of attacks, but "find unregulated app stores" is a tactic that would be unique to the COVID-19 themed malicious apps attack. We also observe that the *exploitation* stage almost always leverages victims' mistrust in social engineering, which highlights that human factor remains to be a critical vulnerability in COVID-19 attacks, which reinforces the importance of seeking effective defenses against such attacks [33].

Insight 2: COVID-19 attacks can be very sophisticated, rather than only opportunistic, which means that effective defense must be designed on a deeper understanding about the attack tactics that can be used in each stage of the attack (i.e., knowing the attacker better).

III. EXPLORING THE DEFENSE SPACE

The preceding characterization of COVID-19 attacks guides us to explore defense strategies against them, with an emphasis on *what-to-leverage* when designing defense systems. The investigation of these proposed approaches is beyond the scope of the present paper. This is because each approach needs to be investigated separately, with corresponding experiments.

A. COVID-19 Malicious Websites Defense

We propose four approaches to defending against COVID-19 themed malicious websites. The first approach is to leverage various website contents pertinent to COVID-19. What is unique to content-based detection of COVID-19 themed malicious websites is the COVID-19 related features, such as the presence or absence of keywords in website names (e.g., *coronavirus*, *COVID-19*, *masks*, *n95*, and *test*). The second approach is to leverage website environment, including URLs' information. For example, we mentioned that attackers may use typo-squatting techniques to make a COVID-19 themed malicious website mimic a legitimate website, highlighting the importance of detecting type-squatted URLs. The third approach is to leverage websites' age information. Since COVID-19 themed malicious websites would be created after the outbreak of the COVID-19 pandemic, hinting that the lifetime of many such websites would be short. The fourth approach is to leverage effective training to make users more skeptical about website contents.

B. COVID-19 Malicious Emails Defense

We propose three approaches to defending against COVID-19 themed malicious emails. The first approach is to filter emails by searching COVID-19 themed keywords in their subject lines and contents. Examples of such keywords include: *COVID-19 cures*, *COVID-19 guidelines*, and *COVID-19 offers*. The second approach is to verify the sender email address to detect email masquerading [34]. The third approach is to leverage email content, for example by analyzing their attachments, links and texts.

C. COVID-19 Malicious Mobile Apps Defense

We propose four approaches to defending against COVID-19 themed malicious apps. The first approach is to leverage computer vision to proactively examine newly published app's logos, especially when they are similar to, if not exactly the same as, the logos of some popular legitimate apps. The second approach is to analyze the content of apps to detect the malicious ones (e.g., repackaged apps). For this purpose, static analysis, dynamic analysis, and their combinations may be utilized. The third approach is to examine the string edit distance of app names with respect to some popular ones. The fourth approach is to train users to improve their awareness of malicious apps according to some best practices in using mobile apps securely [35].

D. COVID-19 Malicious Messaging Defense

We propose three approaches to defending against COVID-19 themed malicious messaging. The first approach is to leverage message content to check if a message contains suspicious content (e.g., the presence of URLs, emoticons, special characters, and COVID-19 themed keywords). The second approach is to detect persuasive messages waging social engineering cyberattacks. This may be achieved by analyzing texts and leveraging human factors and psychological means [33]. The third approach is to train users to improve their awareness of COVID-19 themed malicious messages.

E. COVID-19 Misinformation Defense

We propose four approaches to defending against COVID-19 themed misinformation attacks. The first approach is to use fact-checking to detect fake news (or social media posts), perhaps using similar news reports from credible sources and AI or machine learning techniques. The second approach is to use central repositories to host COVID-19 related information and resources (e.g., Facebook's COVID-19 Information Center). The third approach is to train and educate users to improve their skills and capabilities in recognizing fake misinformation. The fourth approach is to leverage crowdsourcing, namely encouraging or incentivizing users to report COVID-19 suspicious misinformation posts and links.

IV. CONCLUSION

We have explored the landscape of COVID-19 themed cyberattacks and defenses. We discussed 5 classes of attacks and mapped them to the Cyber Kill Chain model. We explored defense strategies against these attacks. Although the study is geared towards COVID-19 themed cyberattacks, the exploration and landscape can be adapted to future X-themed cyberattacks exploiting future events (e.g., election, natural or man-made disasters). It is also interesting to rigorously model these attack-defense interactions in the Cybersecurity Dynamics framework [36]–[39].

REFERENCES

[1] Menlo-Security, "Sophisticated covid-19–based phishing attacks leverage pdf attachments and saas to bypass defenses," https://www.menlosecurity.com/blog/sophisticated-covid-19-based-phishing-attacks-leverage-pdf-attachments-and-saas-to-bypass-defenses, 2020, accessed on 5th June, 2020.

[2] S. Huntley, "Findings on covid-19 and online security threats," https://www.blog.google/threat-analysis-group/findings-covid-19-and-online-security-threats/, 2020, accessed on 5th June, 2020.

[3] P. Upatham and J. Treinen, "Amid covid-19, global orgs see a 148% spike in ransomware attacks; finance industry heavily targeted," https://www.carbonblack.com/2020/04/15/amid-covid-19-global-orgs-see-a-148-spike-in-ransomware-attacks-finance-industry-heavily-targeted/, 2020, accessed on 10 June, 2020.

[4] CheckPoint, "A perfect storm: the security challenges of coronavirus threats and mass remote working," https://www.blog.google/threat-analysis-group/findings-covid-19-and-online-security-threats/, 2020, accessed on 5th June, 2020.

[5] R. McElroy, "What is the cyber security equivalent of washing your hands for 20 seconds?" https://www.enterprisetimes.co.uk/2020/04/15/what-is-the-cyber-security-equivalent-of-washing-your-hands-for-20-seconds/, 2020, accessed on 31st May, 2020.

[6] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," *Leading Issues in Information Warfare & Security Research*, vol. 1, p. 80, 2011.

[7] N. A. Khan, S. N. Brohi, and N. Zaman, "Ten deadly cyber security threats amid covid-19 pandemic," May 2020. [Online]. Available: https://www.techrxiv.org/articles/Ten_Deadly_Cyber_Security_Threats_Amid_COVID-19_Pandemic/12278792/1

[8] M. V. Fontanilla, "Cybercrime pandemic," *Eubios Journal of Asian and International Bioethics*, vol. 30, no. 4, pp. 161–165, 2020.

[9] B. Collier, S. Horgan, R. Jones, and L. A. Shepherd, "The implications of the covid-19 pandemic for cybercrime policing in scotland: a rapid review of the evidence and future considerations," 2020.

[10] R. He, H. Wang, P. Xia, L.-L. Wang, Y. Li, L. Wu, Y. Zhou, X. Luo, Y. Guo, and G. Xu, "Beyond the virus: A first look at coronavirus-themed mobile malware," *ArXiv*, vol. abs/2005.14619, 2020.

[11] H. S. Lallie, L. A. Shepherd, J. R. C. Nurse, A. Erola, G. Epiphaniou, C. Maple, and X. Bellekens, "Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," 2020.

[12] R. Naidoo, "A multi-level influence model of covid-19 themed cybercrime," *European Journal of Information Systems*, pp. 1–16, 2020.

[13] K. Gradoñ, "Crime in the time of the plague: Fake news pandemic and the challenges to law-enforcement and intelligence community," *Society Register*, vol. 4, no. 2, pp. 133–148, 2020.

[14] P. Xia, H. Wang, X. Luo, L. Wu, Y. Zhou, G. Bai, G. Xu, G. Huang, and X. Liu, "Don't fish in troubled waters! characterizing coronavirus-themed cryptocurrency scams," 2020.

[15] T. Brewster, "Coronavirus scam alert: Watch out for these risky covid-19 websites and emails," https://www.forbes.com/sites/thomasbrewster/2020/03/12/coronavirus-scam-alert-watch-out-for-these-risky-covid-19-websites-and-emails/, 2020, accessed on 11 June, 2020.

[16] PrivSec, "Typosquatting duplication of pharmaceutical domain – possibly used for phishing activity," https://gdpr.report/news/2020/05/06/typosquatting-duplication-of-pharmaceutical-domain-possibly-used-for-phishing-activity/, 2020, accessed on 9 June, 2020.

[17] RiskIQ, "Covid-19 cybercrime update," "https://www.riskiq.com/blog/analyst/covid19-cybercrime-update/", 2020, accessed on 3 June, 2020.

[18] S. Singh, "Coronavirus-themed document targets brazilian users," https://www.zscaler.com/blogs/research/coronavirus-themed-document-targets-brazilian-users, 2020, accessed on 10 June, 2020.

[19] S. Gatlan, "Azorult malware infects victims via fake proton-vpn installer," https://www.bleepingcomputer.com/news/security/azorult-malware-infects-victims-via-fake-protonvpn-installer/, 2020, accessed on 5 June, 2020.

[20] Ac, J. Myers, and E. Murphy, "Technical analysis: Hackers leveraging covid-19 pandemic to launch phishing attacks, fake apps/maps, trojans, backdoors, cryptominers, botnets ransomware," https://www.carbonblack.com/2020/03/19/technical-analysis-hackers-leveraging-covid-19-pandemic-to-launch-phishing-attacks-trojans-backdoors-cryptominers-botnets-ransomware/, 2020, accessed on 5th June, 2020.

[21] B. Small, "Scam emails demand bitcoin, threaten blackmail," https://www.consumer.ftc.gov/blog/2020/04/scam-emails-demand-bitcoin-threaten-blackmail, 2020, accessed on 11 June, 2020.

[22] L. W. Schifferle, "Looking for work after coronavirus layoffs?" https://www.consumer.ftc.gov/blog/2020/04/looking-work-after-coronavirus-layoffs, 2020, accessed on 11 June, 2020.

[23] I. Sherr, "Apple, google, amazon block nonofficial coronavirus apps from app stores," https://www.cnet.com/news/apple-google-amazon-block-nonofficial-coronavirus-apps-from-app-stores/, 2020, accessed on 2nd June, 2020.

[24] R. Lemons, "Lessons from the war on malicious mobile apps," https://www.darkreading.com/mobile/lessons-from-the-war-on-malicious-mobile-apps/d/d-id/1333946, 2019, accessed on 3rd June, 2020.

[25] R. Heilweil, "Coronavirus scammers are flooding social media with fake cures and tests," https://www.vox.com/recode/2020/4/17/21221692/digital-black-market-covid-19-coronavirus-instagram-twitter-ebay, 2020, accessed on 11 June, 2020.

[26] Storyful-Intelligence, "Misinformation and disinformation," https://storyful.com/thought-leadership/misinformation-and-disinformation/, 2018, accessed on 5th June, 2020.

[27] E. Barclay, "Why these scientists still doubt the coronavirus leaked from a chinese lab," https://www.vox.com/2020/4/23/21226484/wuhan-lab-coronavirus-china, 2020, accessed on 5th June, 2020.

[28] J. Vincent, "Conspiracy theorists say 5g causes novel coronavirus, so now they're harassing and attacking uk telecoms engineers," https://www.theverge.com/2020/6/3/21276912/5g-conspiracy-theories-coronavirus-uk-telecoms-engineers-attacks-abuse, 2020, accessed on 5th June, 2020.

[29] J. Ross, "Coronavirus outbreak revives dangerous race myths and pseudoscience," https://www.nbcnews.com/news/nbcblk/coronavirus-outbreak-revives-dangerous-race-myths-pseudoscience-n1162326, 2020, accessed on 12 June, 2020.

[30] W. H. Organization, "Coronavirus disease (covid-19) advice for the public: Myth busters," https://www.who.int/emergencies/diseases/novel-coronavirus-2019/advice-for-public/myth-busters, 2020, accessed on 12 June, 2020.

[31] Intermountain-Healthcare, "Debunking common face mask misconceptions," https://intermountainhealthcare.org/blogs/topics/covid-19/2020/07/debunking-common-face-mask-misconceptions/, 07 2020, accessed on 1st August, 2020.

[32] S. R. Christina Farr, "Facebook, amazon, google and more met with who to figure out how to stop coronavirus misinformation," https://www.cnbc.com/2020/02/14/facebook-google-amazon-met-with-who-to-talk-coronavirus-misinformation.html, 2020, accessed on 4th June, 2020.

[33] R. M. Rodriguez, E. Golob, and S. Xu, "Human cognition through the lens of social engineering cyberattacks," *Frontiers in Psychology*, 2020.

[34] S. Baki, R. Verma, A. Mukherjee, and O. Gnawali, "Scaling and effectiveness of email masquerade attacks: Exploiting natural language generation," in *Proc. ACM AsiaCCS*, 2017, p. 469–482.

[35] Y. Magali, "10 security best practices for mobile device owners," https://www.cdillc.com/10-security-best-practices-mobile-device-owners/, accessed on 8 August, 2020.

[36] S. Xu, "Cybersecurity dynamics," in *Proc. HotSoS'14*, 2014, pp. 14:1–14:2.

[37] J. Mireles, E. Ficke, J. Cho, P. Hurley, and S. Xu, "Metrics towards measuring cyber agility," *IEEE T-IFS*, vol. 14, no. 12, pp. 3217–3232, 2019.

[38] Y. Chen, Z. Huang, S. Xu, and Y. Lai, "Spatiotemporal patterns and predictability of cyberattacks," *PLoS One*, vol. 10, no. 5, p. e0124472, 05 2015.

[39] M. Xu, K. M. Schweitzer, R. M. Bateman, and S. Xu, "Modeling and predicting cyber hacking breaches," *IEEE T-IFS*, vol. 13, no. 11, pp. 2856–2871, 2018.