I.J. Information Engineering and Electronic Business, 2021, 2, 1-10
Published Online April 2021 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijieeb.2021.02.01

Cybercrimes during COVID -19 Pandemic

Raghad Khweiled
Palestine Technical University – Kadoorie, Faculty of Graduate Studies, Tulkarem, P.O. Box 7, Palestine
Email: r.f.khweiled@students.ptuk.edu.ps

Mahmoud Jazzar
Palestine Technical University – Kadoorie, Faculty of Graduate Studies, Tulkarem, P.O. Box 7, Palestine
E-mail: m.jazzar@ptuk.edu.ps

Derar Eleyan
Palestine Technical University – Kadoorie, Faculty of Graduate Studies, Tulkarem, P.O. Box 7, Palestine
E-mail: d.eleyan@ptuk.edu.ps

Received: 31 January 2021; Revised: 25 February 2021; Accepted: 07 March 2021; Published: 08 April 2021

Abstract: COVID-19 pandemic has changed the lifestyle of all aspects of life. These circumstances have created new patterns in lifestyle that people had to deal with. As such, full and direct dependence on the use of the unsafe Internet network in running all aspects of life. As example, many organizations started officially working through the Internet, students moved to e-education, online shopping increased, and more. These conditions have created a fertile environment for cybercriminals to grow their activity and exploit the pressures that affected human psychology to increase their attack success. The purpose of this paper is to analyze the data collected from global online fraud and cybersecurity service companies to demonstrate on how cybercrimes increased during the COVID-19 epidemic. The significance and value of this research is to highlight by evident on how criminals exploit crisis, and for the need to develop strategies and to enhance user awareness for better detection and prevention of future cybercrimes.

Index Terms: Cybercrimes, cyber-attacks, malware, COVID-19, work-from-home.

1. Introduction

During the last quarter of 2019, the world started new form of life due to the COVID-19 pandemic. The increasing number of affected socials to nearly 60 million and over one million deaths [1]. Countries had to impose prohibitions and separation between people to decrease infections to save lives and reduce the spread of COVID-19 virus. As a result, computer system and virtual world become essential communication between people. For example, most companies requested their employees to work from home, students moved to online studies, online shopping increased, and social networking activity increased, leading to an increase in Internet users significantly [2].

Although traditional crime rates decreased due to curfews' imposition, cybercrime rates have witnessed a remarkable increase since the beginning of the pandemic. However, cybercriminals exploit the COVID-19 pandemic. As such, they have increased their attacks and focused on campaigns related to COVID-19, such as online selling of unlicensed drugs as cure for the disease, sharing fake news on social media, and sending phishing emails to victims [3]. The aim is to deceive victims in order to get their money or steal their confidential information. Furthermore, they exploit the difficulty of protecting enterprise employees' devices by IT staff when working remotely, especially those personal computers are often less protected than company devices. Attack campaigns also included governments and organizations, for example, the World Health Organization on March 13th recorded attack attempts by an organized group to steal information from the organization employees [4].

The purpose of this paper is to analyzes and compare the data collected from the first half of 2020 with the same period during 2019 to highlight different type of cyberattacks that increased or decreased during the epidemic. The study demonstrates on how criminals can exploit crisis to achieve different type of cybercrimes. In addition, the research articulates on how lack of awareness at user level contributes to the increase of cybercrimes.

This paper is organized as per the following. Next section discusses related cybercrimes and how cybercriminals take advantage of calamities, natural disasters, and epidemics to increase the number of attacks and targets. Subsequently, details and analysis on data collected from companies in the first half of 2020 were discussed. Afterwards, presentation of the types of cybercrimes that have increased dramatically during COVID-19 and comparing them with the first half of 2019 followed by discussion and concluding remarks.

2. Background Work

With the widespread embrace of digital technology, the number of Internet users increased for different purposes, including social interactions, business, and marketing, leading to the emergence of new crimes known as cybercrime. It is expected that losses due to these crimes will reach 10.5$ trillion by 2025 [5]. Cybercrime, also known as "computer-related crime, is any criminal activity that involves a computer either as an instrument, target, or a means for perpetuating further crimes that come within the ambit of cybercrime" [6]. According to Shinder & Cross in [7], cybercrime, like traditional crime, needs three factors simultaneously for crime to occur. These factors are victim, motivation, and opportunity [8]. The victim is the object of the attack, such as the user on social media. Sometimes there is a group of victims, for example, when the attack is on a group of employees in a particular company. The motivation that encourage criminal to commit crime and the opportunity is the criminal exploits to commit crimes. Routine activity theory (RAT) use similar factors to describe the crime [8]. The difference is the absence of a capable guardian, clear cybercrime laws and legislations, and the difficulty of arresting criminals.

With the passage of time and the rapid increase in technology develpoment, the attacker became more experienced and sophisticated in selecting victims in a coordinated manner to increase the likelihood of the attack success. Therefore we have a term known as opportunistic attacks [9]. Opportunistic attacks can be assumed as attacks focus on selection of victims based on the most vulnerable victim [9,10]. In other words, attackers search for gaps or weaknesses in the company's system, making it more vulnerable to attack. Moreover, they are looking for victims who have weaknesses to sustain successful cyber attacks. This weakness may be due to the victim's psychological state (such as anxiety, panic), which helps the attackers succeed. Therefore, they are using social engineering to be able to lure and deceive the victim. For example, when employees are under pressure at work, they become more anxious and fearful. As such, when receiving phishing emails by impersonating their manager, they may not be able to verify geniun emails; this triggers most malicious links and confidential information misuse. There are other factors that opportunistic attackers take advantage to increase their profits and campaigns' success, including exploiting ongoing crises, important public events, natural disasters and epidemics [9,11]. In natural disaster attacks, opportunistic attackers pretend to be legitimate or trusted bodies such as charities or government organizations to communicate with disaster victims to deceive them and give them confidential information or volunteers to persuade them to donate money [11]. For example, during 2005 Hurricane Katrina caused significant damage in New Orleans and nearby areas in the States [12]. Later, Hurricane Katrina websites appeared inviting people to donate to the disaster victims, which later turned out to be fraudulent sites aimed at deceiving volunteers and stealing their money [13]. More in 2014, fraudsters took advantage of Ebola pandemic outbreak to open phishing emails to lure people or donate money to fake organizations [14]. In November of 2014, more than 700,000 spam emails were revealed asking people to donate to fight Ebola by pretending they were donation campaigns led by Indiegogo fundraiser [15]. As we have seen, attackers exploit any incident or epidemic for advantage in oder to make their campaigns successful. As such, it was not surprising that they used the COVID-19 pandemic as advantage by exploiting people's fear of infection. For instance, nearly 200,000 coronavirus-related threats were recorded in seven days during March 2020, some related to email phishing [16].

Next section discuss on cyberattacks and cybercrimes that increased during COVID-19 pandemic and how successful campaigns increased by cybercriminals as result of psychological exploitation and pressures exposed dure to the pandemic.

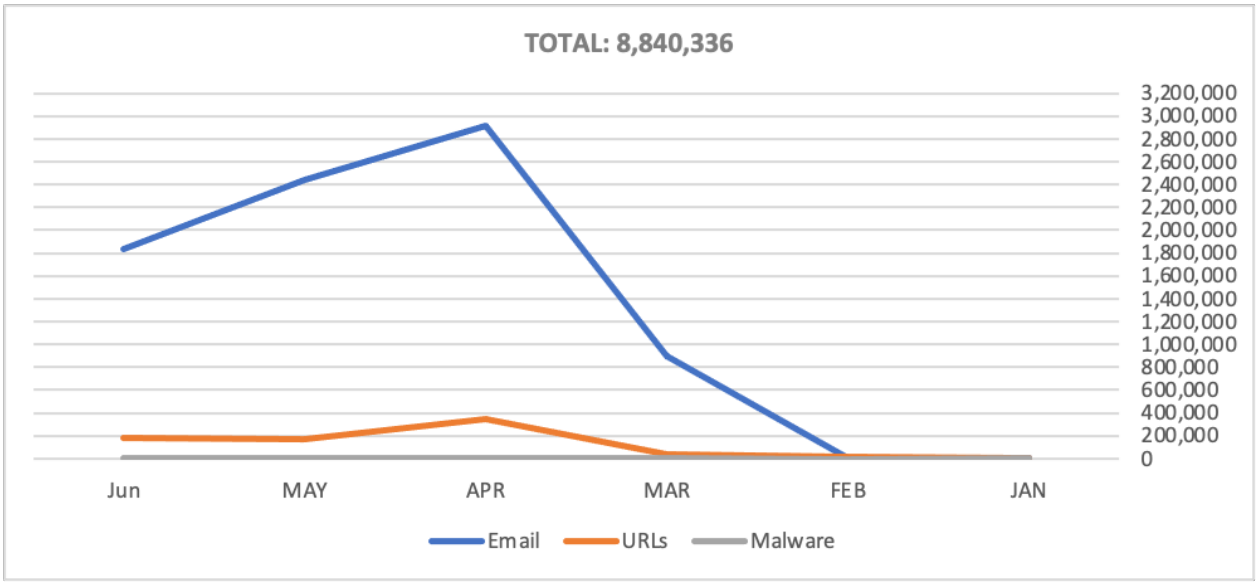

Fig.1. Types of threats related to COVID-19

3. Cybercrimes during COVID-19 Pandemic

Due to the emergence of noticeable increase in cybercrimes during the COVID-19 pandemic, most information security companies and international organizations have embarked on studying and identifying cybercrime types that have increased, such as Trend Micro company, Interpol, and Anti-Phishing Working Group (APWG) [17,3,19]. We have classified Cybercrime in COVID-19 pandemic into threats related to COVID-19, the most vulnerable countries, and cybercrime types that emerged during the pandemic.

3.1. Threats Related to COVID-19

According to Trend Micro [17], 8,840,336 threats related to the COVID-19 were detected in the first half of 2020, with most of the discoveries occurring in April, coinciding with the pandemic's peak in most countries around the world. As shown in Figure 1, these threats consist of emails threats, URLs threats, and Malware threats, which refer directly to the epidemic (such as websites that publish fake news about the epidemic) or indirect (such as emails that indicate delay in the order due to the curfew).

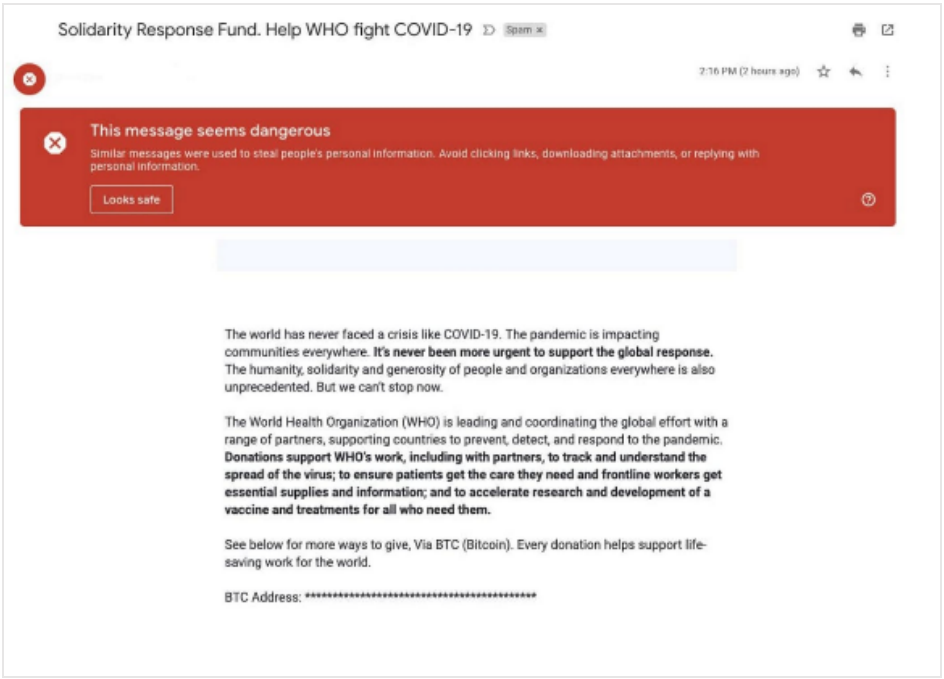

Fig.2. Example of an email impersonating the world health organization (WHO) [33].

Emails are considered as one of the most used tools, as it is used in phishing campaigns, spear phishing, spamming, spreading fake news, fraud, and Fake donation campaigns [17]. Moreover, emails are considered as the most official communication media between companies and employees, so cybercriminals take advantage of this circumstance to increase their campaigns. Figure 2 is an example of an email impersonating the World Health Organization (WHO) intended to request fraudulent donations to COVID-19 patients. Most of the URLs that were registered as a threat belong to phishing scams, such as exploiting people sitting at home and posting offers for a free Netflix subscription on social media App (Facebook or Twitter). The post contains a malicious link; when clicked; the victim will be transferred to a fake Netflix login page designed to capture their login credentials [17]. They also use websites to promote applications that they claim to protect their users from the Coronavirus. It has been shown that they infect users' devices with a hypothetical virus called: BlackNET RAT. This tool adds the affected device to a botnet used for DDoS attacks, stealing the Firefox cookies, saved passwords, and Bitcoin wallets [18]. As discussed, malware threats were detected during the first half of 2020. One of the most common examples is the appearance of a trojan called QNodeService sent via a fake email shown as tax exemption notice due to COVID-19 from United States government to deceive the victim. Trojans stole the victim's credentials from Chrome and Firefox browsers and managed data on victims' devices [17].

3.2. Countries Most Vulnerable to Threats

United States is one of the countries that has been observed as the most threatened by different forms of cyberattacks. According to the INTERPOL report [3], the most reported cybercrimes are fraud and theft of sensitive information through phishing campaigns that target employees who work remotely. Campaigns includes ransomware targeting small and medium companies, exploitation focuses on the increasing use of social media, child sexual exploitation and more. The United Kingdom, Germany, France, and European countries, have reported a noticeable increase in the malicious domain related to the COVID-19 epidemic. For instance, the word corona in the second-level domain to deceive people searching for information about the epidemic. The spread of ransomware campaigns in health and government sectors, impersonation of websites related to government agencies, and using it in phishing campaigns [3]. MENA region which is considered among others in Figure 3 has recorded a noticeable increase in disseminating fake news about COVID-19 epidemic in social media. In addition to the emergence of malicious domains that refer to counterfeit statistical sites about coronavirus and the increase in fraud campaigns, online selling of unlicensed drugs as a cure for the disease [3].

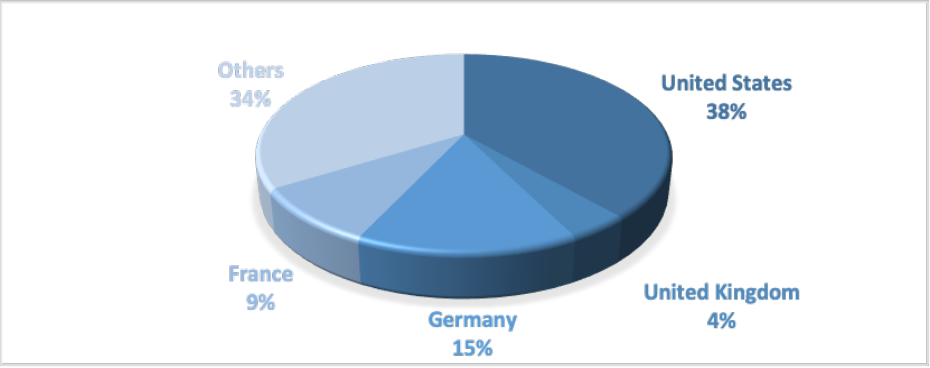

Fig.3. Countries threat distribution in H1 of 2020.

3.3. Types of Cybercrimes

The first half of 2020 witnessed noticeable increase in various types of cybercrimes contain phishing, ransomware, spread of misinformation, distributed denial of service, and trojans.

3.3.1. Phishing

Phishing is considered one of the most common cybercrimes. Phishers take advantage of fear of the virus and the curiosity to find out information about it such as the number of confirmed cases and mortality, disease symptoms, and possible treatment methods to established successful phishing campaigns [3]. According to APWG report [19], 267,372 phishing campaigns were reported in H1 of 2020, increasing (19.06%) over 2019 during the same period. As shown in Figure 4, these campaigns targeted different sectors such as SaaS/email, financial institutions, payment, and social media.

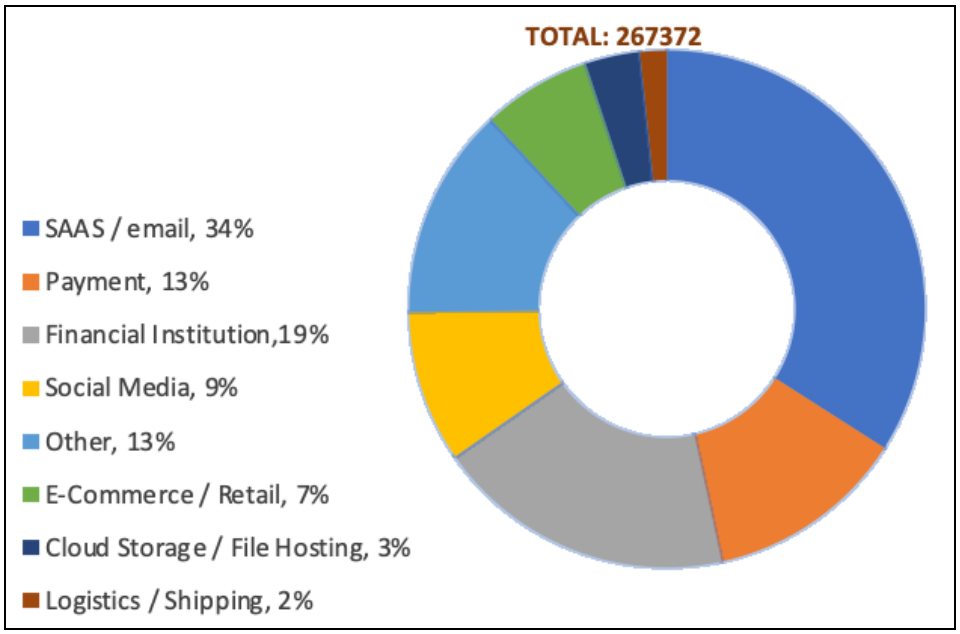

Fig.4. Sectors targeted by phishing campaigns in H1 of 2020.

Victims were deceived by pretending that the message was from the national or global health authorities, governments, offers of vaccines and medical supplies, urging charitable donations related to COVID-19 [3]. As example, Figure 5 presents a phishing email which has been sent to specific employees pretending to be from company management.

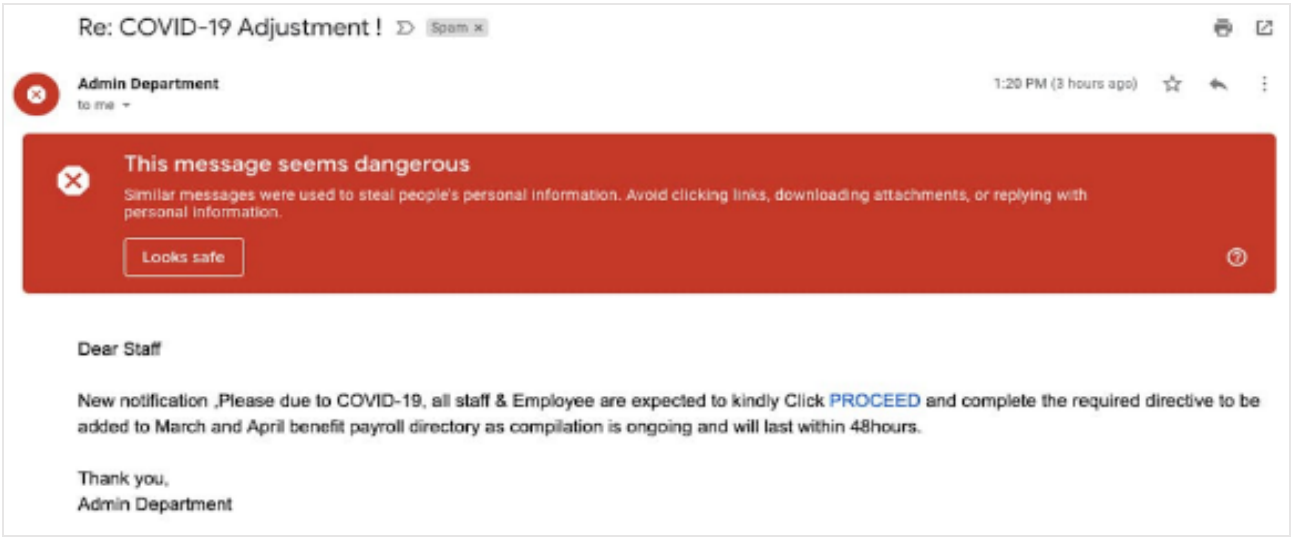

Fig.5. Example of phishing email [33].

As illustrated in Figure 6 below, March witnessed the highest number of phishing sites discover [20]. The domains of some phishing sites that were detected contained "COVID" and "Corona" [2], thus deceiving people who are looking for sites designed to spread information on coronavirus.

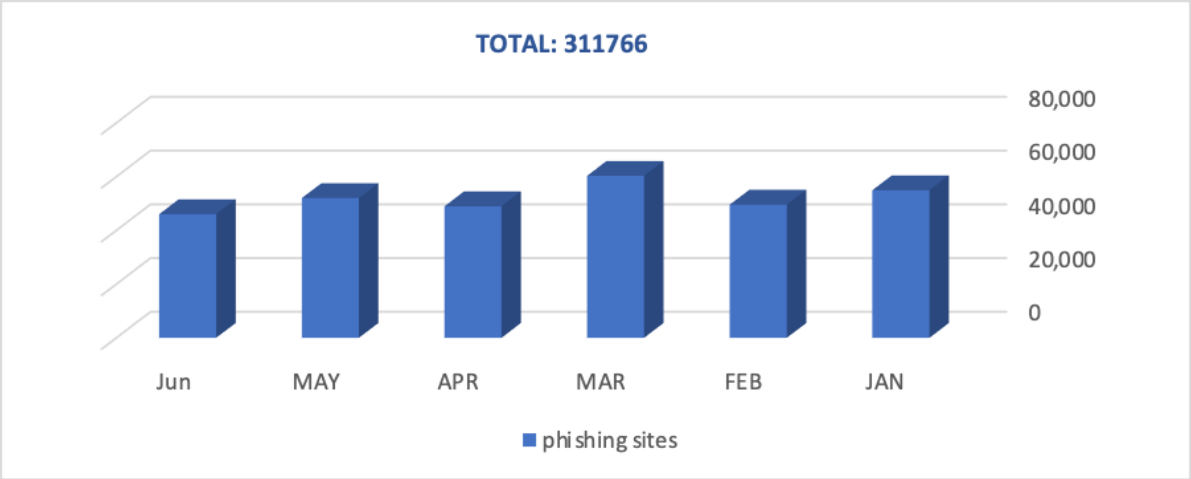

Fig.6. Distribution of phishing sites detected in H1 2020.

3.3.2. Ransomware

The first half of 2020 witnessed significant decrease in detecting ransomware attacks, including files, URLs, and email. Despite its decline, there was an increase in losses due to higher ransom demands, and the cost of growing remediation [21]. According to the coalition report [21], "the average ransom increased (100%) from 2019 through Q1 2020 and increased 47% from Q to Q2 2020". Therefore, due to the targeted organizations sensitivity, most organizations were forced to pay ransom, even if it was high. As per Trend Micro reports [17] and as demonstrated in Figure 7 below, healthcare was the second most targeted organization. It is the most fragile component of the infrastructure in countries where the COVID-19 pandemic is prevalent. For example, some hospitals have been forced to pay ransoms to the cybercriminal to avoid losing patient lives [9].

People fear of infection and spread of the epidemic has led to new ransomware families. As such, 68 new families have been uncovered [22]. Most of the discovered malwares belongs to campaigns which target users searching for websites or applications related to coronavirus. For example, the DomainTools security research team discovered a website that attracts users to download an Android app that aims to track the heatmap of COVID-19, later it was found that the app is ransomware which is capable to locks the user screen for the sake of ransom [23].

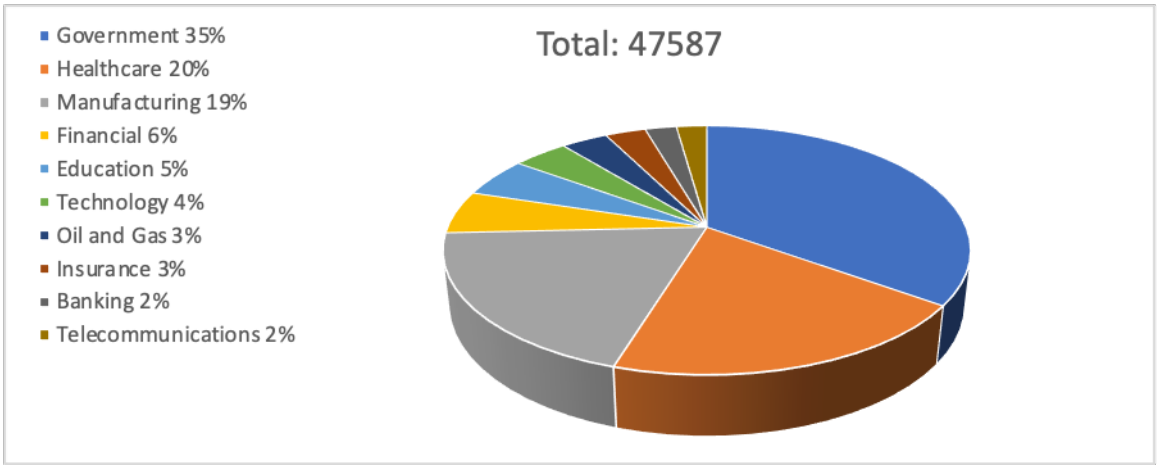

Fig.7. Top industries targeted by ransomware files detected in H1 2020.

3.3.3. Spread of Misinformation

Since the beginning of the epidemic late 2019, misinformation has started to spread in various media, including traditional media, websites, and social media. Social media had the most significant impact on spreading misinformation and fake news more quickly. Facebook report posted warning signs to nearly 50 million of the misinformation posts related to COVID-19 in April; Twitter warned that more than 1.5 million users are spreading misinformation and fake news related to the epidemic during the same month [24]. The fake news included misinformation about how to treat, miracle cures, claims that coconut oil kills the virus, and drugs with no proven

clinical benefit that are nonetheless described as useful. Moreover, spreading the news about conspiracy theories such as the virus is being created as biological weapon, and other fake and misleading news [25,26].

3.3.4. Distributerd Denial of Service

February 2020 witnessed the largest distributed denial of service (DDoS) attacks. Amazon Web Services reported that an unidentified customer on their network was attacked by 2.3 Tbps and lasted up to 3 days using a technology called Lightweight Offline Access Protocol [27,28]. This technique uses vulnerable third-party servers and raises the volume of data sent to the victim's IP address by 56 to 70 times [27,28]. According to Neustar Report [27], there was increase in the number of DDoS attacks detected in H1 2020 as compared to the same period in 2019. In contrast, Netscout report [29] showed that the number of DDoS attacks detected in H1 of 2020 was 4.83 million, where the increase was estimated at (27.1%) over 2019 during the same period. The epidemiological situation and the infrastructure's weakness in the health, educational, and economic sectors worldwide were exploited to increase the attacks. As shown in Figure 8, an increase in detected attacks in North America (NA), Laten America (LATAM), and in Europe, the Middle East, and Africa (EMEA) region. Turkey is one of the countries that faced high attacks during H1. Although the increase is general, there was a decrease in the number of detected attacks in Asia Pacific (APAC) region. Nevertheless, that attacks have focused on the eCommerce and health sectors.

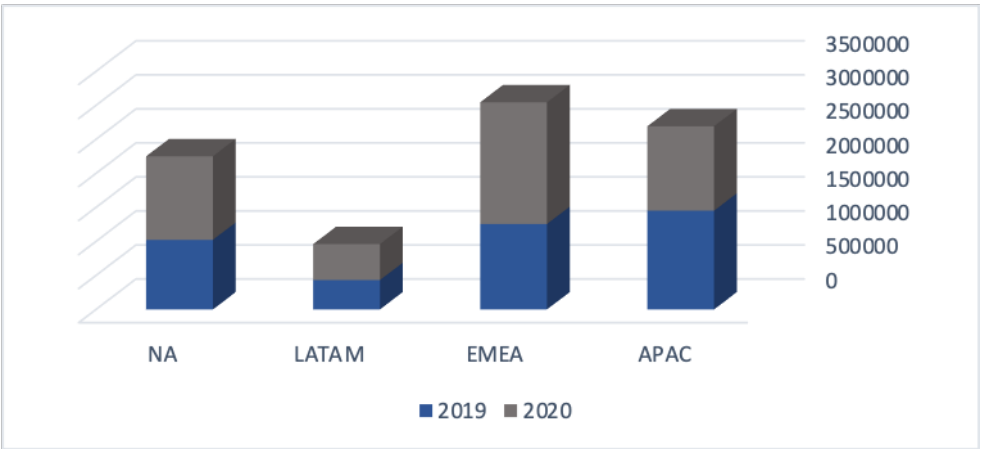

Fig.8. Number of DDoS attacks by region 1H 2019 vs 1H 2020.

3.3.5. Sunburst Trojans

By the end of the year 2020, FireEye's major cybersecurity company discovered the most dangerous and largest hacking operation globally [30,32]. FireEye reported that it had been breached for hacking tools used to test computer defense [30]. Later, emerged that FireEye hack was part of larger attack carried out by professional hackers. FireEye revealed on December 13 that SolarWinds' Orion software update caused the attack [30,31]. SolarWinds customers were asked to update the Orion software using the company page, later, hackers removed the page after news of the attack were spread. More than 18,000 employees updated the software, thinking it was from the original company.

According to FireEye, the hack was carried out by a group of Russian hackers (APT29) who breached the infrastructure of the SolarWinds system [31,32]. Once a customer signs in to request an update, APT29 can install the update that contains Trojans; later named as Sunburst. To avoid detection, the attackers modified a legitimate utility on the Orion system with malicious components to be used as legitimate components before they returned the legitimate utility. The size of the losses, the sectors, and the targeted countries has not been entirely determined. FireEye report stated that "the victims included governmental, advisory, technical, communications and extractive entities in North America, Europe, Asia, and the Middle East" [31]. Never the less, the development of proactive monitoring systems and best practices contribute to minimize threats and defense against cyber-attacks [33]. In addition, risk assessment and cybercrime laws contribute to controls and defend organizations for combating cybercrimes at national and international level [34,45].

Table 1. Comparison of Cybercrimes in H1 of 2019 and H1 of 2020

Cybercrime	Count in H1 of 2019	Count in H1 of 2020	Relative change (%)
Phishing campaign	224556	267372	+19.06%
Ransomware	46,177,026	14,594,852	-68.4%
DDoS	3800000	4830000	+27.1

4. Concluding Remarks

The analyses indicate clear and noticeable increase in cyber-attacks and cybercrimes at the peak of COVID-19 epidemic worldwide. Due to the imposition of bans by governments and the stay at homes, this led to an increase in the use of the Internet and thus the exploitation of cybercriminals to increase their campaigns. As shown in Table 1 above, the increase was in phishing due to phisher's exploitation of the pandemic and the increase of their campaigns related to COVID-19 directly such as messages related to donations for the benefit of COVID-19 patients, or indirectly such as emails that indicate delay in the order due to the curfew.

The significant increase in DDoS as attacks on governments, health, and economic sectors intensify. Although the significant decrease was clearly noticed in the recorded ransomware attacks, there was an increase in losses due to higher ransom demands, and the cost of remediation is growing. In addition, a remarkable increase in the spread of misinformation and fake news found a fertile environment in social media. Furthermore, towards the end of 2020, the world witnessed the discovery of the biggest hacking attacks and hence the discovery of the most dangerous and largest hacking operation. Sunburst Trojans were published, pretending to be the updated software.

The outcome of this research demonstrates by evident an increase of the cybercrimes in government and private sectors during COVID-19 due to the lack of distinguished low level security measures and the lack user awareness. Therefore, thoughtful measures should be considered by governments and organization leaders to increase the level of cyber security during any abnormal conditions, development of more sophisticated proactive cyber-attack detection software, and to activate firm ICT monitoring during any unprecedented and emergency conditions is indispensable.

Acknowledgment

The authors wish to thank Palestine Technical University-Kadoorie (PTUK) for supporting this research work as part of PTUK research fund.

References

[1] WHO, “WHO Coronavirus Disease (COVID-19) Dashboard,” https://covid19.who.int/, Retrieved July 13, 2020.
[2] R. Naidoo, “A multi-level influence model of COVID-19 themed cybercrime,” *Eur. J. Inf. Syst.*, vol. 29, no. 3, pp. 306–321, May 2020, doi: 10.1080/0960085X.2020.1771222.
[3] Interpol, “Cybercrime : Covid-19 Impact,” https://www.interpol.int, Retrieved July 18, 2020.
[4] T. Seals, “WHO Targeted in Espionage Attempt, COVID-19 Cyberattacks Spike | Threatpost,” https://threatpost.com/who-attacked-possible-apt-covid-19-cyberattacks-double/154083/, Retrieved July 18, 2020.
[5] S. Morgan, “Cybercrime To Cost The World $10.5 Trillion Annually By 2025,” https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/, Retrieved July 18, 2020.
[6] M. Chawki, A. Darwish, M. A. Khan, and S. Tyagi, *Cybercrime,Digital Forensics and Jurisdiction*, SCI, Volume 593, 2018.
[7] D. L. Shinder and M. Cross, *Scene of the Cybercrime*, Burlington, MA: Syngress Pub., 2008.
[8] R. W. Taylor, E. J. Fritsch, and J. Liederbach, *Digital Crime and Digital Terrorism*, 3rd ed., Pearson, 2015.
[9] R. W. Taylor, E. J. Fritsch, and J. Liederbach, *Digital Crime and Digital Terrorism*, 3rd ed., Pearson, 2015.
[10] J. R. C. Nurse, “Cybercrime and you: How criminals attack and the human factors that they seek to exploit,” *arXiv*, 2018, doi: 10.1093/oxfordhb/9780198812746.013.35.
[11] K. Tysiac, “How cyber criminals prey on victims of natural disasters,” https://www.journalofaccountancy.com/news/2018/sep/cyber-criminals-prey-on-natural-disaster-victims-201819720.html, Retrieved December 13, 2020.
[12] FBI, “Hurricane Katrina Fraud,” https://www.fbi.gov/history/famous-cases/hurricane-katrina-fraud, Retrieved Nov. 28, 2020.
[13] FBI, “FBI Cyber Executive Warns of Hurricane Katrina Scams,” https://archives.fbi.gov/archives/news/stories/2005/september/katrina_scams091405, Retrieved Nov. 28, 2020.
[14] CISA, “Ebola Phishing Scams and Malware Campaigns ,” https://us-cert.cisa.gov/ncas/current-activity/2014/10/16/Ebola-Phishing-Scams-and-Malware-Campaigns, Retrieved Nov. 29, 2020.
[15] M. Korolov, “Scammers move from Ebola phishing to fundraising | CSO Online,” https://www.csoonline.com/article/2848481/scammers-move-from-ebola-phishing-to-fundraising.html, Retrieved Dec. 28, 2020.
[16] Cybertalk, “Nearly 200,000 coronavirus themed threats in 7 days - CyberTalk.org,” https://www.cybertalk.org/2020/05/14/nearly-200000-coronavirus-themed-threats-in-7-days/, Retrieved Nov. 28, 2020.
[17] TrendMicro, “Securing the Workplace Trend Micro 2020 Midyear Cybersecurity Report,” https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/securing-the-pandemic-disrupted-workplace-trend-micro-2020-midyear-cybersecurity-report, Retrieved Nov. 28, 2020.
[18] ThreatIntelligenceTeam, “Fake ‘Corona Antivirus’ distributes BlackNET remote administration tool,” https://blog.malwarebytes.com/threat-analysis/2020/03/fake-corona-antivirus-distributes-blacknet-remote-administration-tool, Retrieved Nov. 28, 2020.
[19] APWG, “Phishing Activity Trends Report in Q1 of 2020,” Available: https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf., Retrieved Dec. 12, 2020.

[20] APWG, "Phishing Activity Trends Report in Q2 of 2020." Available: https://docs.apwg.org/reports/apwg_trends_report_q2_2020.pdf., Retrieved Dec. 12, 2020.
[21] Coalition Inc., "Cyber Insurance Claims Report," Available: https://www.coalitioninc.com/blog/coalition-releases-new-2020-cyber-insurance-claims-report, Retrieved Dec. 13, 2020.
[22] TrendMicro, "QNodeService: Node.js Trojan Spread via Covid-19 Lure," https://blog.trendmicro.com/trendlabs-security-intelligence/qnodeservice-node-js-trojan-spread-via-covid-19-lure/, Retrieved Dec. 5, 2020.
[23] T. Saleh, "CovidLock Update: Deeper Analysis of Coronavirus Android Ransomware," https://www.domaintools.com/resources/blog/covidlock-update-coronavirus-ransomware, Retrieved Dec. 23, 2020.
[24] U. Bangkok, "Fake news' in the time of COVID-19," https://bangkok.unesco.org/content/press-provides-antidote-fake-news-time-covid-19, Retrieved Dec. 24, 2020.
[25] S. Evanega, M. Lynas, J. Adams, and K. Smolenyak, "Coronavirus misinformation: quantifying sources and themes in the COVID-19'infodemic'," Available: https://allianceforscience.cornell.edu/wp-content/uploads/2020/10/Evanega-et-al-Coronavirus-misinformation-submitted_07_23_20-1.pdf, Retrieved Dec. 24, 2020.
[26] G. Pennycook, J. McPhetres, Y. Zhang, J. G. Lu, and D. G. Rand, "Fighting COVID-19 Misinformation on Social Media: Experimental Evidence for a Scalable Accuracy-Nudge Intervention," *Psychol. Sci.*, vol. 31, no. 7, pp. 770–780, 2020, doi: 10.1177/0956797620939054.
[27] Neustar, "Cyber threats & trends: JAN-JUN 2020," Availabe: https://www.cdn.neustar/resources/whitepapers/security/neustar-cyber-threats-trends-report-2020.pdf, Retrieved Dec. 23, 2020.
[28] SecurityExpert, "Top Five Most Infamous DDoS Attacks - Security Boulevard," https://securityboulevard.com/2020/09/top-five-most-infamous-ddos-attacks/, Retrieved Dec. 23, 2020.
[29] Netscout, "NETSCOUT Threat Intelligence Report - Cybercrime: Exploiting A Pandemic," https://www.netscout.com/blog/netscout-threat-intelligence-report-1H2020, Accessed: Dec. 23, 2020.
[30] E. Nakashima and C. Timberg, "Russian hacker group 'Cozy Bear' behind Treasury and Commerce breaches - The Washington Post," Available: https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html, Accessed Dec. 24, 2020.
[31] L. Constantin, "SolarWinds attack explained: And why it was so hard to detect," https://www.csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html, Accessed Dec. 24, 2020.
[32] BBCNews, "US cyber-attack: US energy department confirms it was hit by Sunburst hack," https://www.bbc.com/news/world-us-canada-55358332, Accessed Dec. 24, 2020.
[33] N. Kumaran and S. Lugani, "Protecting against cyber threats during COVID-19 and beyond," https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond, Accessed Dec. 13, 2020.
[34] A. A. Süzen, "A Risk-Assessment of Cyber Attacks and Defense Strategies in Industry 4.0 Ecosystem," International Journal of Computer Network and Information Security, Vol.12, No.1, pp.1-12, 2020.
[35] Q. A. Ul Haq,"Cyber Security and Analysis of Cyber-Crime Laws to Restrict Cyber Crime in Pakistan," International Journal of Computer Network and Information Security, Vol.11, No.1, pp.62-69, 2019.

Authors' Profiles

Raghad Khweiled awarded high honor degree in computer information systems from Jordan University of Science and Technology, Irbid-Jordan, 2018. She is currently pursuing graduate degree of science in cybercrimes & digital evidence analysis at Palestine Technical University – Kadoorie. Her research interest includes cybercrime mitigation, cyber-attacks detection, and forensic analysis.

Mahmoud Jazzar is currently working as an assistant professor in computer science and director of the academic quality department at Palestine Technical University – Kadoorie. He served as director of Kadoorie center for innovation in teaching and learning during 2017 – 2018. Prior working at Palestine Technical University - Kadoorie, Jazzar worked as Dean with Royal University for Women in the Kingdom of Bahrain and Assistant Professor in Computer Science with Al-quds University, Curtin University of Technology-Sarawak, and Birzeit University. Jazzar is a member of IEEE Computer Society, IAENG, MySEIG, and the Malaysian Information Technology Society (MITS). He joined many organizing and technical program committees and as a reviewer of many international conferences and journals. His main research lies in the area of Computer and Network Securities, Intrusion Detection and Protection, Forensics, and Intelligent Systems. He has supervised several research projects, published one book and several scientific research papers in his research domain.

Derar Eleyan has a good relevant diversity experience in academic and industry. He is the manager of the Erasmus+ project “Pathway in forensic computing” and associate professor in information systems. Eleyan is currently working as the president assistant for international academic cooperation. He served five years as an assistant professor at Birzeit University in the Department of Computer Science teaching variety of courses at the undergraduate and postgraduate levels. He has worked also as lecturer and course team leader in computing at Southeast Essex college of Arts and Technology where he taught various modules as, information system, project management, database, web database, and website management, Computer and Business Ethics, Research methods. He has a good expertise as an Information Systems Consultant at BAS Computer Systems a private company since 2003 till 2006. In 2006, He was a visiting lecturer at the University of Manchester, teaching an MSc course of Enterprise System Modelling, collaborating with Prof. Loucopoulos. He has served as an external reviewer to some conferences in information science, information systems and business process modelling. His research interests focus on System dynamics, software quality, Information Systems, Business Process Modelling, Customer service and satisfaction and return on investment, information technology management, IT project management, Quality of Service, Academic quality and performance evaluation, Business and computer ethics, Software testing quality assurance, Usability and e-commerce. He is a member of some societies as British Computer Society (BCS), Institute for Learning (IFL), Systems Dynamics Society (SDS).

How to cite this paper: Raghad Khweiled, Mahmoud Jazzar, Derar Eleyan, "Cybercrimes during COVID -19 Pandemic", International Journal of Information Engineering and Electronic Business(IJIEEB), Vol.13, No.2, pp. 1-10, 2021. DOI: 10.5815/ijieeb.2021.02.01