LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 5 issue 2 Year 2021

Cyber Security and COVID-19 Pandemic

Muhammad Shairoze Malik*
13beemmalik@seecs.edu.pk
National University of Science and Technology Islamabad

Abstract:
This paper investigates the issues arisen as a result of COVID-19 pandemic in the domain of cyber security. Vulnerable people and systems have become a target of cyber criminals due to pandemic. This paper discusses an increase in cyber-attacks due to pandemic. Furthermore, the rate of cyber-attacks has been increased due to an increase in fear and anxiety caused by the pandemic. Healthcare organizations have become the primary targets of cyber-attacks during the pandemic. Many companies are expecting employees to work from home (WFH), which has also prompted concerns about cybersecurity and the risk of state-sponsored assaults, and a rise in ransomware and phishing attacks. This paper also offers many practical ways to minimize the dangers of cyber-attacks, while working from home. And also discusses mitigation of healthcare security concerns. It is critical that healthcare companies establish a comprehensive cybersecurity strategy to strengthen the security of their critical data and assets.

Keyword: Pandemic, Cyber-Security, Phishing, Scamming, Malware Attacks, Denial of Service.

1. Introduction

The COVID-19 epidemic has resulted in major problems and has significantly changed our way of life. Organizations have had to adapt by focusing on the remote working of employees on a massive scale and at a rapid speed. Many businesses have been required to update their working environments as well as take decisions that were made in a rush to allow workers to operate from home with no basic preparation or arrangements. A large number of these organizations and groups have no plans in place to deal with such an issue in a short period of time [1]. In actuality, just 38% of organizations have an internet security plan [1]. Organizations and associations all over the globe have recognized the work-from-home (WFH) strategy by switching to a decent web-based environment which generally increases dangers to business data with increasing attack vectors. It is important to emphasize that WFH must become the new standard for people from one end of the planet to the other. Frequently, this entails asking employees to use their own devices and home WiFi-networks, which are usually unsafe due to the absence of critical company standard security defenses. Organizations that currently provide devices to their employees do so with little or no administrative rights, which leads to problems when the user is required to install the needed software. As a result, companies should provide substantially more fair arrangements in addition to giving workers stronger rights, implying significantly higher possible security concerns. Network security during the COVID-19 is a particularly worrisome issue because of growing cyber-treats targeting network frameworks and vulnerable people all over the world [2]. This article focuses on network security concerns that may have arisen due to this global crisis.

2. Literature Review

Online crimes such as fraud provide the highest profits while posing the least danger to the perpetrators under typical circumstances. Examining the facts, it is apparent that more individuals are currently unemployed, spending more time at home, and utilizing the internet for both work and socializing. Furthermore, government officials have provided monetary incentives to residents as well as other companies trying to recruit or retain customers. Because the world is waiting for a feasible solution to prevent the spread of COVID-19, any material pertaining to "COVID-19" will undoubtedly get the attention of normal internet users. Scammers are using this route to transmit harmful online attacks to internet users by impersonating government employees, tax authorities, and so on, as well as links to seek help with COVID-19 [3].

In a recent study, World Economic Forum emphasized that phishing and hacking have become a new normal as it continues to effect systems even after the viruses have been wiped off [4]. Because vulnerable people are more anxious and awaiting emails, text messages, phone calls, and other contacts from authorities over COVID-19 due to which these scams are far more successful now because of pandemic. It has much easier for cybercriminals to create fake websites or messages that appear to be from familiar and relevant authorities, incorporating urgency to capitalize on the widely felt fear factor due to their increasing awareness of people vulnerabilities. As a result, the effectiveness of phishing attacks has gotten a huge boost. It can take various forms, including internal and external updates, personal investments and charities. In a recent F-Secure study, spam is categorized as one of the most common methods for malware to spread. It also highlighted how epidemic is being utilized by attackers to entice users to click, particularly by disguising the executable in organize files systems such as .zip files [5]. It must be considered that criminal actors may use genuine publications as bait to attract people to perform a high-risk activity, such as clicking on a website link or opening a large file. Before proceeding, users should investigate the sender of an email as well as any links contained within it. Cybercriminals regularly employ impersonation methods, such as posing as the WHO (World Health Organization), the UN (United Nations), or a well-known organization, such as Zoom or Microsoft to trick victims into opening infected material or clicking on links.

The whole world has been placed under lockdown due to COVID-19. The shift to a new way of working in which employees frequently work from home, mostly utilizing home equipment protected by their corporate employers, has generated numerous concerns in the sector. As a consequence of this unique mass quarantine agreement, new concerns about the resilience of scientific solutions to various ecosystems are critical; particularly, the strength of current technology within employers' current cyberinfrastructures.

3. Cyber Security Concerns Associated with the COVID-19 Pandemic

3.1 Types of Cyber-Attacks:

Malwares, distributed denial-of-service and Scams & Phishing attacks are the three types of cyber-attacks that occurred during the pandemic (DDoS). Table 1 shows several examples of cyber-attacks during this crisis. APT (Advanced Persistent Threat) groups and Cyber-criminals [6, 7] are using COVID-19 related frauds and phishing to launch cyber-attacks on vulnerable persons and businesses for a variety of reasons, including financial gain or the collection of information about COVID-19 vaccinations. Hades, APT-C-09 Patchwork (aka Dropping Elephant), Hades, APT29 [9] and TA505 [8] are examples of APT activity during the epidemic.

- ✓ Scams and phishing: These are the most successful and most common attacks used in COVID-19 [10, 11]. These attacks have a success rate of 30 percent or more. This is significant because an attacker just need a small number of clicks to get financial or other benefits. As a result, sending millions of email messages to victims requesting financial assistance from the federal government, their businesses, banks, and so on will yield rapid and significant results. There are several phishing attempts (email, SMS, and voice) that target susceptible persons and systems and utilize the term coronavirus or COVID-19 to entice victims [10, 11]. There was a 600 percent rise in coronavirus-related phishing email attacks in the first quarter of 2020 [12]. Cybercriminals are also using more sophisticated techniques to lure victims, such as the use of HTTPS encryption technologies on their websites. SSL is often associated with around 73% of phishing websites [11]. SaaS (Software as a Service) users and webmail users are the most commonly phished [11].

- ✓ Viruses, Trojans, RATs, spyware, worms and ransomware are collectively known as Malwares [13]. Throughout the outbreak, APT groups and cybercriminals took advantage of the crisis by disseminating various forms of malware to vulnerable persons and systems via email messages and websites. In reality, 94 percent of malware-infected PCs were targeted via e-mail. Specific forms of adware and spyware [14], like ransomware, will undoubtedly be more effective for pandemic response groups (Table 1).

- ✓ DDoS (Distributed-Denial-of-Service) Attack: Due to ease of launch and its effect on victim, DDoS is often regarded as the most indefensible cyber-attack. A DDoS attack employs many attack sources to launch a coordinated DoS attack on one or more targets, therefore boosting attack power and complicating countermeasures [15]. During the pandemic, UK's university students and staff were unable to access university's services and the internet due to a DDoS attack on JISC, the UK's university's Web service provider. Furthermore, it is critical to note that healthcare organizations all around the world are being undermined by DDoS attacks (see Table 1).

Type of Attack	Country	Date	Details of Attack
Distributed Denial-of-Service	France	March	A network of hospitals in Paris were affected by DDoS attacks as they were unable to connect to data and email servers [18].
Distributed Denial-of-Service	US	March	DDoS attacks were conducted on US Department of Health and Human Services [18].
Ransomware	UK	March	Medical and personal information of former patients of a medical research firm based in London were leaked by Maze Ransomware Gang [17].
Ransomware	Czech Republic	March	The whole IT network of The Brno University Hospital was forced to shut down by cyber-attacks [16].
Phishing	Taiwan	May	Emails containing RAT (Remote Access Tools) urged public to get tested for COVID-19 by impersonating Taiwan's senior Infection-Disease Control official [19].
Ransomware	US	June	Cybercriminals known as Netwalker forced The University of California, San Francisco (UCSF), which was working on the COVID-19 vaccine, to pay $1.14 million with the help of ransomware attack [20].
Phishing	Germany	June	Emails with intent to sell PPEs (Personal Protective Equipment) were sent to top officials at a firm, which included phishing URLs that took them to fake login sites to steal their credentials [20].
Ransomware	Canada	June	CryCryptor ransomware in form of COVID-19 Contact tracing App were deployed on Android smartphones [22].

TABLE 1: Cyber-attacks in year 2020 during COVID-19)

3.2 Effects on Healthcare Organizations

During the pandemic, one of the primary targets of attacks was the healthcare industry. The attacks against healthcare institutions have highlighted the issues with cybersecurity infrastructure in the healthcare industry. These include pharmaceutical businesses, and research groups as well. WannaCry ransomware assault that rendered the National Health Service (NHS) inoperable in 2017 is one example of cyber-attacks on health service providers. One of the primary reasons is that owing to restricted resources, these organizations must defend their IT systems since they are financed by cities or nations that generally have extremely stringent financial constraints. Obsolete no longer supported software and operating systems such as Windows 7 or Windows XP are being used throughout hospitals to control medical devices. According to Europol, healthcare facilities have become profitable target for ransomware as it is easily accessible. IoT (Internet of Things) devices and computers are widely used to monitor and store patient data in modern hospitals as well as to operate ventilators and ICUs (Intensive Care Units).

CISA, United States DHS and UK's NCSC issued a joint advisory paper and guidelines which discusses concerns such as malwares, phishing, WFH tools such as Zoom, and so on [10]. APT organizations are expected to continue targeting healthcare and vital services throughout the world [23]. Canada's CSE (Communications Security Establishment) and NCSC, in a recent joint report, suggested that the APT29 (aka "Cozy Bear") cyber-attacks being conducted on various organizations which are involved in the development of a COVID-19 vaccine in Canada, US and UK, are done by Russian Intelligence Services with the goal of stealing information related to vaccines [9]. To accomplish its objectives, APT29 employs a variety of tactics, including vulnerability scanning, public exploits, and phishing to obtain access to the target network, as well as proprietary malware known as 'WellMess' and 'WellMail' [9].

3.3 Techniques for Mitigation

There are practical measures that may be used to decrease the danger of cyber-attacks when working from home, but mitigating and avoiding cyber-attacks is not an easy process. Some mitigation techniques are as follows [1, 10, 23]:

- ❖ Virtual-Private-Network (VPN): It is an encrypted communication channel to ensure secure data transmission between two places on the internet. VPNs are being widely used to access internet these days. It provides integrity and secrecy, and it enables companies to extend security standards to WFH employees.
- ❖ Educating Users: Many security systems consider people to be the weakest link. As a result, raising awareness about cyber-attacks among users through ongoing training is critical to reducing the risks. Just 11% of firms have offered cybersecurity training to non-cybersecurity staff in the last year, according to a recent survey [24].
- ❖ Two-Factor-Authentication: It provides increased security by requiring an OTP (One Time Password) code given to your mobile phone through SMS or an authentication app along with login username and password. It helps in preventing brute force attacks as well as password guessing and theft, as well as. Two factor authentication should be implemented between organization's network and an employee working from remote location to verify their identity.

- Anti-Malware Software’s: Cybercriminals use numerous forms of malware to attack susceptible victims. Because millions of new malware and strains are created each year, using frequent and up-to-date anti-malware may minimize the danger of malware-based cyber-attacks.
- Firmware Updates: All devices' and equipment's firmware/OS should be up-to-date with the most recent security patches. It may decrease the danger of a latest vulnerabilities and zero-day assaults.
- Segmentation and Separation: Divide a network into trustworthy zones such as the Internet zone (untrusted), the entertainment network (low trust level), the home office network (high trust level) and avoid using a single network for all types of communication. A separate Wi-Fi should be implemented for the working of IoT devices which can help in limiting the security exposure of the network infrastructure and can help in containing breaches.
- Robust Corporate Online Policy: To safeguard data and prevent cyber-attacks, a robust and comprehensive policy is required as organizations have had little or no time to prepare for the remote working situations. Strong WFH rules include not having critical business discussions in public, only using company approved audio and video conference lines, and so on. A recent research found that 46% of organizations only test their recovery and backup strategies once a year or less, so a proper recovery plan and backup method should also be included in the policies and it is also critical to evaluate these plans on a regular basis [25].
- Physical-Security: It is critical to secure home office electronics physically. Measures include not leaving work computers alone, locking the laptop or using a lock screen, always logging-off after usage, and so on.

4. Discussion

Primary focus of on-gong cyber-attacks have been the healthcare organizations, which are working to resolve COVID-19. It is critical that these companies should strengthen their defenses against cyber-attacks in order to safeguard their important data and assets. Security Incident and Event Management along with a proper Intrusion Detection Systems (IDS) are two critical components for identifying hostile conduct that might make a network vulnerable to cyber-attacks. An IDS normally use three types of techniques to make an evaluation of cyber-threats: Signature matching, Anomaly detection, Deep packet inspection. Or it uses a mixture of all three approaches to create a hybrid system. IDS which make use of Artificial Intelligence (AI) is becoming increasingly popular as they have the ability to identify zero-day assaults more precisely. It is also critical for healthcare companies to have a holistic approach to cybersecurity, seeing security not only from a technology standpoint, but also within the context of procedures [26]. Risk Management, CERT-RMM (CERT Resilience Management Model) [27] and making cybersecurity a part of strategic planning and allocating a proper budget to it [26] are all examples of comprehensive approaches to cybersecurity.

5. Conclusion

The cybersecurity problems encountered during the COVID-19 outbreak have been explored and examined in this article. The most significant cyber-attacks and vulnerabilities are identified and summarized. Potential mitigating techniques and ways to reducing the dangers of cyber threats are also explored. APT-groups and cyber criminals have been attacking vulnerable individuals and systems by taking advantage of the epidemic. This scenario is unlikely to alter in the near future. Healthcare companies have been among the most targeted by cybercriminals during the epidemic for a variety of reasons. As a result, it is critical that healthcare companies enhance their defenses against cyber-threats such as implementing a holistic strategy to cybersecurity.

6. References

[1] Furnell S, Shah JN. Home working and cyber security–an outbreak of unpreparedness? Comput Fraud Secur. 2020; 2020(8): 6- 12.

[2] Hakak S, Khan WZ, Imran M, Choo KKR, Shoaib M. Have you been a victim of COVID-19-related cyber incidents? Survey, taxonomy, and mitigation strategies. IEEE Access. 2020; 8: 124134- 124144.

[3] Aleroud A, Zhou L. Phishing environments, techniques, and countermeasures: a survey. Comput Secur. 2017; 68: 160- 196.

[4] Anti-Phishing Working Group. The APWG phishing activity trends report 1st quarter 2020. https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf. Accessed July 9, 2020.

[5] Sattler J. COVID-19 scams — how to spot and stop coronavirus email attacks. https://blog.f-secure.com/re-covid-19-scams-how-to-spot-and-stop-coronavirus-email-attacks/. Accessed June 24, 2020.

[6] Alshamrani A, Myneni S, Chowdhary A, Huang D. A survey on advanced persistent threats: techniques, solutions, challenges, and research opportunities. IEEE Commun Surv Tutor. 2019; 21(2): 1851- 1877.

[7] Xiao L, Xu D, Mandayam NB, Poor HV. Attacker-centric view of a detection game against advanced persistent threats. IEEE Trans Mobile Comput. 2018; 17(11): 2512- 2523.

[8] Malwarebytes. APTs and COVID-19: how advanced persistent threats use the coronavirus as a lure. https://resources.malwarebytes.com/files/2020/04/200407-MWB-COVID-White-Paper_Final.pdf. Accessed August 27, 2020.

[9] National Cyber Security Centre (NCSC) and Communications Security Establishment (CSE). Advisory: APT29 targets COVID-19 vaccine development. https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf. Accessed July 17, 2020.

[10] National Cyber Security Centre (NCSC) and Cybersecurity and Infrastructure

Security Agency (CISA). Advisory: COVID-19 exploited by malicious cyber actors. https://www.ncsc.gov.uk/news/-covid-19-exploited-by-cyber-actors-advisory;. Accessed June 4, 2020.

[11] World Economic Forum. COVID-19 risks outlook - a preliminary mapping and its implications. http://www3.weforum.org/docs/WEF_COVID_19_Risks_Outlook_Special_Edition_Pages.pdf. Accessed June 9, 2020.

[12] Sjouwerman S. Q1 2020 coronavirus-related phishing email attacks are up 600%. https://blog.knowbe4.com/q1-2020-coronavirus-related-phishing-email-attacks-are-up-600. Accessed August 30, 2020.

[13] Crown Prosecution Service. Cybercrime - prosecution guidance. https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance. Accessed: July 11, 2020.

[14] Arabo A, Pranggono B. Mobile malware and smart device security: trends, challenges and solutions. Proceeding of the 19th international conference on control systems and computer science. New Jersey: IEEE; 2013: 526- 531.

[15] Asri S, Pranggono B. Impact of distributed denial-of-service attack on advanced metering infrastructure. Wireless Pers Commun. 2015; 83(3): 2211-2223.

[16] Cimpanu C. Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak. https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/. Accessed July 20, 2020.

[17] Goodwin B. Cyber gangsters hit UK medical firm poised for work on coronavirus with Maze ransomware attack. https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-lorganisation-poised-for-work-on-Coronavirus. Accessed July 20, 2020.

[18] Hale G. DDoS attacks on rise due to COVID-19. https://www.controleng.com/articles/ddos-attacks-on-rise-due-to-covid-19/. Accessed July 20, 2020.

[19] Lyngaas S. ‘Vendetta’ hackers are posing as Taiwan's CDC in data-theft campaign. https://www.cyberscoop.com/vendetta-taiwan-coronavirus-telefonica/. Accessed July 20, 2020.

[20] Lyngaas S. Hackers target senior executives at German company procuring PPE. https://www.cyberscoop.com/germany-ppe-coronavirus-hackers-ibm/. Accessed July 20, 2020.

[21] Tidy J. How hackers extorted $1.14m from University of California, San Francisco. https://www.bbc.com/news/technology-53214783. Accessed July 20, 2020.

[22] Osborne C. New ransomware masquerades as COVID-19 contact-tracing app on your Android device. https://www.zdnet.com/article/new-crycryptor-ransomware-masquerades-as- covid-19-contact-tracing-app-on-your-device/. Accessed July 20, 2020.

[23] National Cyber Security Centre (NCSC) and Cybersecurity and Infrastructure Security Agency (CISA). Advisory: APT groups target healthcare and essential services. https://www.ncsc.gov.uk/news/apt-groups-target-healthcare-essential-services-advisory. Accessed June 4, 2020.

[24] Pedley D, Borges T, Bollen A, et al. Cyber security skills in the UK labour market 2020–Findings report. Department for Digital, Culture, Media and Sport. 2020. https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020/cyber-security-skills-in-the-uk-labour-market-2020

[25] Malecki F. Overcoming the security risks of remote working. Comput Fraud Secur. 2020; 2020(7): 10- 12.

[26] Bhuyan SS, Kabir UY, Escareno JM, et al. Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. J Med Syst. 2020; 44: 1- 9.

[27] Caralli R, Allen J, White D, Young L, Curtis P. CERT Resilience Management Model Version 1.2. https://resources.sei.cmu.edu/asset_files/Handbook/2016_002_001_514462.pdf. Accessed August 28, 2020.