International Journal of Computer Trends and Technology
ISSN: 2231 – 2803 / https://doi.org/10.14445/22312803/IJCTT-V69I1P108

Volume 69 Issue 1, 38-40, January 2021
© 2021 Seventh Sense Research Group®

Review Article

The Impact of COVID-19 on Cyber Security

Mohammed A Aljama [1], Fadi Alsafwani [2]

[1,2] Saudi Aramco Company, Information Technology, Saudi Arabia

Received Date: 04 December 2020
Revised Date: 16 January 2021
Accepted Date: 19 January 2021

Abstract *- Coronavirus Disease 2019 (COVID-19) has had a huge impact on societies and individuals. The outbreak has introduced a global health challenge. In addition, the pandemic has exposed dynamic cybersecurity threats, and privacy challenges to business organizations and individuals. This paper will compare internet usage before and after COVID-19 to understand its role in evolving cyber-attacks. This paper aims to provide an analysis of some of the most common threats that increased or evolved during the pandemic, along with recommendations to be taken to overcome those threats. This paper will also discuss why education is the most important element and the first line of defense in preventing cyber threats.*

Keywords *- VPN, Malware, Phishing, COVID-19, Vulnerability, Video calls.*

I. INTRODUCTION

The COVID-19 pandemic has been the most talked-about subject worldwide in the last first half of 2020. This is not surprising as COVID-19 touched people around the world. The pandemic forced organizations and individuals to adapt to new practices, such as social distancing, wearing masks, and washing hands. It touched the way we have fun and connected with family and other people and changed the way we work. As organizations make a huge shift in how work is done, whether temporarily or permanently, many vulnerabilities and cyber weaknesses surface, and cybercriminals capitalize and take full advantage of this crisis. As much as we care about our health during this pandemic, it is very important to also care about the safety of organization's or individual's information from destruction or being stolen, as this will most likely create a crisis of its own. To understand how cyber-attacks differed after the pandemic, it is important to examine the cause that led cybercriminals to focus on this type of attack.

II. NETWORK USAGE DIFFERENCE

A big network usage shift caused by the COVID-19 pandemic has been the exponential growth in voice and video traffic. The popularity of text, whether in chat, emails, or social media posts, has always been superior to voice and video calls. As the coronavirus spreads, governments require people to stay at home, and public and private organizations are asking employees to work remotely. In the United States, VPN usage grew 49% since the COVID-19 crisis. Video calls have risen by 36%, while voice calls are up by 25% (Branscombe, 2020). The amount we are spending on or how we are using the internet has changed, but the time we use it is different. Before COVID-19, the peak time of using the internet was between 5 p.m. and 11 p.m., and now usage has doubled, and the peak time is from 8 a.m. to 11 p.m. globally (Branscombe, 2020). This means as long as the majority of people are awake, it is peak time.

Table 1.

Country	**COVID-19 cases increase per week**	**VPN usage increase per week in %**
Italy	51,768	160
United States	33,005	124
Spain	28,094	58
Germany	23,833	40
Iran	15,072	49
France	14,809	44
Switzerland	7,142	12
United Kingdom	5,405	18
Russia	400	57

VPN Usage Increase in countries with most COIVD-19 Cases between March 8-22, 2020 (Clement, 2020)

III. COVID-19 THREATS LANDSCAPE

These network usage changes, combined with the health anxiety spread among people, have allowed hackers to leverage some known cyber-attacks that each organization must be prepared for.

A. VPN Threats

With the rapid move to working remotely from home, virtual private networks (VPNs) have become critical in companies. Based on a survey on 300 Korean enterprises, about 45% of large enterprises have practiced teleworking through VPN after the COVID-19 outbreak, against 9.7% before the outbreak (OECD, 2020). The sudden and urgent need for VPNs, combined with organizations' unpreparedness, increases the probability of misconfiguring VPNs, which might lead to exposing sensitive information. This also exposes organizations to some other threats, such as Denial of Service Attacks. Another threat comes from using personal computers to perform business duties in the corporate network, as not all companies offer business PCs to their employees. Using policy unrestricted personal computers exposes corporate networks to a wide range of risks, such as data leakage, spyware/viruses infection, and lower malware defense. Before organizations jump to a conclusion of accepting the risk of using VPNs, they should take serious measures and invest some time and money to strengthen their VPN servers. The main focus should be on three points: authorization management, sensitive information exposure, and malware protection. Authorization validation measures should be in place to ensure all VPN connections are completely validated and equipped with valid certificates to prevent any compromise to the network.

The Recommendation: Organizations should also assess the option of providing corporate-owned and security managed laptops to employees. This investment will eliminate being exposed to many risks, which will ensure no sensitive data is leaked and no malware-infected devices are connected to the corporate network. While this option seems costly initially, the cost of having risks associated with employees connected using their laptops is much higher.

B. Phishing Emails

Email phishing attacks have spiked over 600% since the end of February 2020 due to the pandemic (Sharma, 2020). Criminal hackers are taking full advantage of the pandemic by spreading Coronavirus-themed emails, pretending to be a government organization, Ministry of Health, or any trustworthy source, to convince people to reveal their personal information. The main purpose of phishing attacks is to insert malware into the network. Malware could be info-stealers, ransomware, or RATS (Remote Access Trojans), allowing hackers to control or monitor victims' computers. Organizations need to step up the awareness of phishing emails, as such malicious emails could have a huge impact on the organization's security. To highlight how big the issue is, Google recently blocked 18 million phishing emails related to COVID-19 in just one week (Davis, 2020). Cyber Criminals always try to manipulate people emotionally, and they know how COVID-19 messages trigger emotions. Hackers try to be as creative as possible when choosing the email subject to maximize the believability. Malicious email subjects include:

- Claim your Free Facemasks and thermometers
- Apply for COVID-19 Government Financial Aid
- Coronavirus Test Results

The Recommendation: Organizations should start utilizing technologies and solutions that filter incoming emails and block them before reaching employees' inboxes. Of course, many external emails will have to be allowed, as most organizations deal with external entities daily. This is where human awareness comes into play. Organizations intensify spreading the awareness among employees and equip them with ways to identify external and potential emails that have a high probability of being suspicious, then teach employees how to deal with these emails. Employees should be trained to create strong passwords, report phishing emails, and use data correctly.

C. Ransomware Attacks

Ransomware is a type of malware that cybercriminals usually deploy or use against critical organizations. Ransomware allows attackers to encrypt all information and block access to files on infected systems or networks. Access to files cannot be restored unless a ransom or financial gain is paid by the victim. Recent observations by INTERPOL, the International Criminal Police Organization, showed that there had been a spike of ransomware attacks against IT networks of hospitals and health organizations due to the increase of their criticality during the pandemic (Interpol, 2020). There has also been a noticeable spike in specific ransomware attack techniques. Research has shown that Remote Desktop Protocol (RDP) access attacks have become the most popular attack technique used by attackers during the current pandemic due to many employees and students working remotely (Oberly, 2020). The second most common way to infect systems with ransomware is via phishing emails that contain malicious links that lead the employee to run an executable containing the attacker's exploits. Other techniques mainly capitalize on finding vulnerabilities, bugs, or glitches in some organization services, such as a public-facing application and VPN network.

The Recommendation: Since the main means to transmit ransomware in a system is via phishing emails, all discussed preventive measures and recommendations to defend against such malicious emails must be applied. Organizations' systems must be scanned, assessed, and patched regularly for potential bugs or vulnerabilities that might allow attackers to break through and exploit ransomware.

IV. BEST PRACTICES & PREVENTIVE MEASURES

There are some generic and basic, yet important, best practices that should be adopted, especially during the rise of cyber-attacks during the pandemic. These practices are categorized into the following: Prevention, Detection, and Response.

A. Education & Awareness (Prevention)

Cybercriminals are leveraging that people are even more fearful and anxious and try to capitalize on people's negligence to conduct attacks. Companies must continue to empower and educate employees to stay vigilant. Creating a cyber-awareness culture in the organization requires an enormous effort, as it involves changing behavior.

One of the most important and challenging elements is how an organization can measure success. In other words, how can an organization prove that the behavior of its employees has changed and became more vigilant to cyber-attacks? One of the most common and yet effective tools is utilizing phishing training. Phishing simulations can give a measurable insight into how security awareness is reflected in online behavior. Companies should not rely solely on this technique, but it gives a fairly good indication of how well employees are educated when they know how to deal with phishing emails. Typically, a company with a good security awareness program will have around only 4% of its employees failing phishing tests (Goodwin, 2020). To have effective cybersecurity in an organization, every individual has to be an active player.

B. *Patch software constantly (Prevention)*

Keeping your software up-to-date is the most essential, yet most basic, activity that should in place all the time. As cyber-attacks evolve every day, software like antiviruses and network device firmware should all be equipped with patches to counter these new exploits. Organizations should install updates as soon as they become available.

C. *Conduct Vulnerability Assessments & Penetration Tests (VAPT) (Prevention)*

A good indicator that an organization is taking cybersecurity seriously is the existence of vulnerability assessments and Penetration Tests (VAPT) regular practice, whether done by the company’s red team or third-party external entity. VAPT activity with the right advanced tools will give a huge insight into the organization's network security standing by revealing existing vulnerabilities and exploits that attackers could use.

D. *Monitor User Permissions (Detection)*

As employees are being laid off due to budget cuts and revenue losses in many companies, many former employees leave while their permissions and authorizations to a company’s vital systems stay. This increases the possibility of illegal data breaches and could initiate cyber-attacks from unhappy former employees. Regular review and audit of user permissions and users with high privileges can prevent a huge risk to the organization’s network

E. *Monitor Network Activity (Detection)*

An intrusion Detection System (IDS) should be deployed to monitor network activity to mark any unusual traffic. Attackers often try to paralyze organizations by launching Distributed Denial of Service Attacks (DDoS), which causes downtime for the whole network, resulting in economic losses. With a larger number of employees working from home, attackers have tailored DDoS to attack VPN networks.

F. *Ensure Regular Backups Availability (Response)*

Organizations must sustain backups at regular intervals to recover from any successful attack on the organization’s digital data. Backups should be tested regularly and stored offsite.

G. *Ensure Regular Backups Availability (Response)*

Many companies have Business Continuity Plans (BCPs), but few have considered including an infectious disease outbreak as one of the predicted scenarios since such incidents rarely happen on a global scale. Now that we have experienced it, such a crisis should no longer be ignored and must be included in BCPs. These plans should be updated and practiced in drills to test response efficiency. Business Continuity enablers should not contradict strategies imposed by cybersecurity professionals, and rather they should align with them. To increase the level of preparedness, BCPs and BIAs need to scale up, not just include incidents but also outbreaks. For example, if BCP or BIA is considering small scale security events requiring a limited number of employees to work from home, the risk is small. If outbreaks require a majority of people to work from home, then the attack surface increases dramatically. There should be a balance and risk analysis to what level of risk is accepted while ensuring the business's continuity. Many companies will have to depend on third-party communication applications.

V. CONCLUSION

Covid-19 has impacted the way we live and work. During the pandemic, the amount and type of network usage have changed. Hence cybercriminals adjusted their type of attacks to increase their rate of success. Organizations should apply and deploy security tools and software to prevent the most common attacks in this pandemic. More importantly, organizations should educate their employees, as investing in security awareness is less expensive than the cost of a cyber-attack or security breach. Organizations must prepare response plans to ensure business continuity in cyber incidents and then apply lesson-learned activities to prevent similar future incidents.

REFERENCES

[1] Branscombe, Mary., The Network Impact Of The Global COVID-19 Pandemic. (2020) [online] The New Stack. Available at: <https://thenewstack.io/the-network-impact-of-the-global-covid-19-pandemic/>

[2] Clement, J., COVID-19 And VPN Usage Increase In Selected Countries As Of (2020) [online] Statista. Available at: <https://www.statista.com/statistics/1106137/vpn-usage-coronavirus/>, graph.

[3] Organization for Economic Co-operation and Development, OECD Economic Surveys: Korea 1st ed. OECD Publishing, (2020)120.

[4] Sharma, S., Watch Out! Phishing Attacks Around Coronavirus Spike By Over 600%. (2020) [online] NewsBytes. Available at: <https://www.newsbytesapp.com/timeline/science/59291/276821/coronavirus-themed-phishing-attacks-spike-by-667>

[5] Davis, J., Google Blocks 18M Daily COVID-19-Related Phishing Emails. (2020). [online] HealthITSecurity. Available at: <https://healthitsecurity.com/news/google-blocks-18m-daily-covid-19-related-phishing-emails>

[6] Interpol., Cybercriminals Targeting Critical Healthcare Institutions With Ransomware. (2020) [online] Available at: <https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware>

[7] Oberly, David., Strategies For Combating Increased Cyber Threats Tied To Coronavirus. [online] The Daily Swig | Cybersecurity news and views. (2020). Available at: <https://portswigger.net/daily-swig/strategies-for-combating-increased-cyber-threats-tied-to-coronavirus>

[8] Goodwin, Matthew., Phishing Awareness - The More They Know, The Less The Threat. (2020) [online] Cyber Defense Magazine. Available at: <https://www.cyberdefensemagazine.com/phishing-awareness-the-more-they-know-the-less-the-threat/>