International Journal of Future Generation Communication and Networking
Vol. 14, No. 1, (2021), pp. 1626–1632

Cyber Security Threats Post COVID-19

Mr. Rakesh L. Patil
Asst. Professor,
Tilak Maharashtra Vidyapeeth, Pune
Email: rakesh@tmv.edu.in

Ms. Asmita Namjoshi
Asst. Professor,
Tilak Maharashtra Vidyapeeth, Pune
Email: asmita03@gmail.com

Abstract:
'History Repeats', In 2008 economic slowdown cybercriminals launched the cyberattacks on individuals as well as corporate. COVID-19 is also no exception for cyber attacks. Cybercriminals are using technical knowledge with social engineering methods to launch sophisticated attacks. Findings from Readsmith show that in the early stages of COVID-19 scams have increased by 400 % and criminals are taking full advantage of this situation. Cybercriminals know peoples are searching for safety information and they are more likely to fall into the trap laid by them, with the quarantine policy forcing companies to make an unprecedented transition to work from home policy, the atmosphere created by the pandemic helped cybercriminal and cons artist thrive. In this research paper; subsequent subject areas are discussed - Introduction to Cyber Security, Cyber Attacks related to COVID-19, and countermeasures.

Keywords: *COVID-19, Cyber Security, Cyber Criminal, ATO (Account Take Over attack), Botnet, Bots, Megakart Attack, Browser Web, Mobile Phishing, Mobile Threats.*

I. Introduction:

Opportunistic criminals are taking advantage of the COVID-19 coronavirus pandemic to launch a variety of cyberattacks. According to a McAfee threat report released in November 2020, cyber-attacks have seen a massive surge in Q2 of 2020 because of Covid-19. Detection of cyberattacks grew by 605% in Q2. [1] Cybercriminals had used different techniques including credential phishing, malicious attachments and links, business email compromise, fake landing pages, downloader's, spam, malware and ransomware strains, and phone scams. In a Pandemic situation, most people are dependent on e-commerce, these peoples have fallen victim to phishing scams where they ordered safety devices or instruments, and the product was never delivered to them. Further cybercriminals have been reported for stealing banking credentials from the elderly by pretending them as they are helping in the pandemic.

Another impact of Covid-19 is seen on the education Institution. Due to the pandemic situation, many countries decided to close the education institutes including schools, colleges, and universities. Considering the student's future lectures, assignments and examinations are conducted online on a very large scale but in an untested and unprecedented state. [2] Students, Teachers, and corporate employees had to be shift from the physical workplace to the virtual workplace, this increases the demand for video conferencing app for educational, personal, and business use. In March video conferencing apps as Google meet, Microsoft Team, and Zoom saw 62 million downloads. Zoom was one of the most downloaded app globally for video conferencing in February and March and it continues to see a high number of downloads across the US, EU, and the UK. [3]

The organization has to deal with growing security demands emerging from cyber attacks. As the business are transforming new system challenges and priority are increasing such as real-time decision making, online staff training, continuity risk, and mainly cyber attacks. [2] To meet this situation organization has to deal with growing security demands and keep the sensitive data and privacy of the people who might be infected due to Covid-19. For example, during pandemic situation a massive

ISSN: 2233-7857 IJFGCN

increase in Zoom app also exposed the growing list of security flaws. User email address and photo leaked, a flaw found in zoom installer allows an attacker to gain root access to computers that run malicious version. These security flaws result in a ban & restrict the zoom by companies and government agencies. Some of the companies like Google, SpaceX, and Smart communication had banned Zoom including government and government agencies like NASA, USA Senate, Australian Defense force, etc. [4]

II. Statistics of cyber attacks during Covid-19

According to the report published by Microsoft Detection and Response Team (DART) in the first two weeks of April 2020, multiple ransomware groups activated dozens of ransomware deployment. [5] The report published by IBM states that remote work impacts the average cost of a data breach of $137 thousand. The cost of a data breach is highest in the healthcare sector which was $7.13M in the year 2020. [6]

In Gartner survey conducted on 14th April 2020 states that cybersecurity and data breach is the most increased third party risk that emerged in their organization. [7] Due to the pandemic situation organization relying on the remote workforce has more risk to expose the organization to unsecured practices. This survey has also revealed that 52% of legal and compliance leaders are concerned about the risk that arises due to Pandemic.

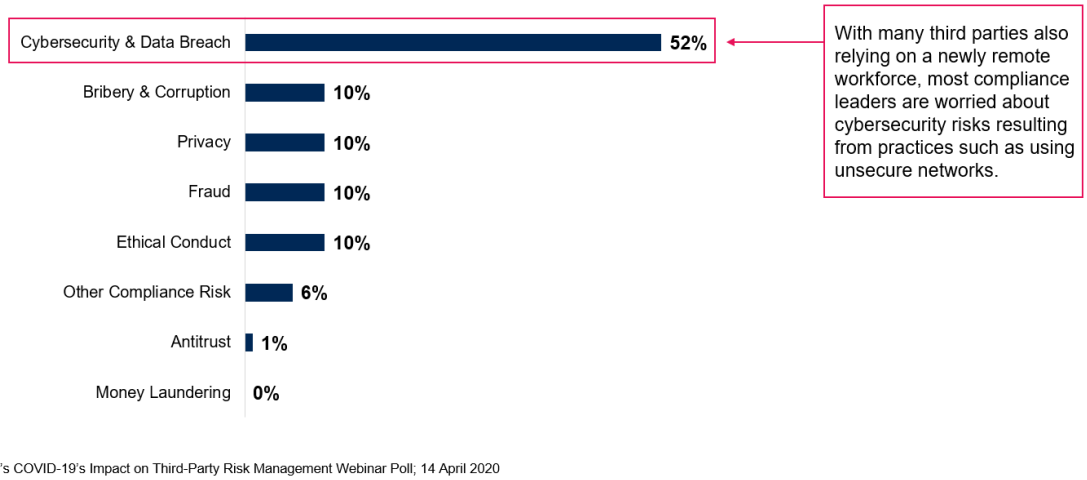

Figure 1: Third party risks most organization faced during COVID-19? [7]

According to the report published by Skybox Security Ransomware growth surge to 72% and mobile vulnerability surge to 50%. [8] This report also states that 77 ransomware campaigns were observed during the first few months of the pandemic which have targeted several mission-critical research labs and healthcare companies. [8]

According to the report published by Verizon, 85% of mobile phishing happens outside of email apps. 96% of mobile users have installed other communication or social media apps on their phones and organizations are giving up on mobile security and putting everyone at risk.[9]

Lookout's Apurva Kumar and Kristin Del Rosso said nearly 4,000 people fells victim to the attack in which the cybercriminals created more than 200 fake websites of the bank before banks got aware of his attack. [9] Mobile phishing situation is rising because it is very difficult to spot an attack due to the limitation of a small screen and the use of short URLs. Figure2 shows the instances that malicious URLs are accesses during the Covid-19 pandemic.

ISSN: 2233-7857 IJFGCN

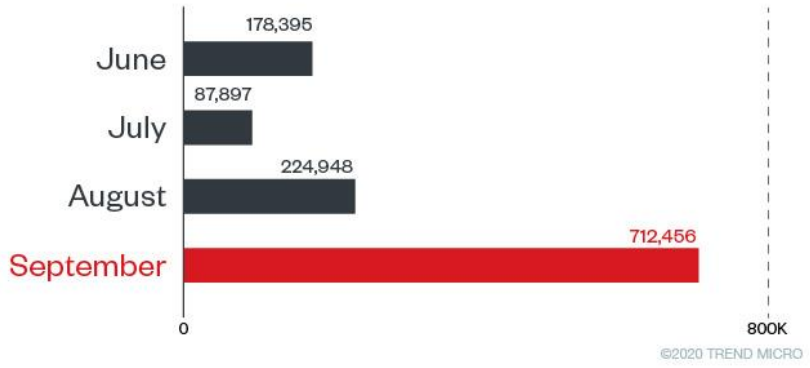

Figure 2: Instances that accessed malicious COVID-19 related URLs [10]

According to a report published by Panda Security, Covid-19 scam victims from the UK have lost £11 million collectively till 8th July 2020. FBI & CISA reported that the people's republic of China targeting the intellectual property of Covid-19 research organizations. Brno University Hospital is targeted for cyberattack in The Czech Republic. From January to July total of 2,16,001 attacks were seen in the Asia-Pacific region. United States has the highest country average cost of $8.64 M for data breach attacks.[11]

III. Cyber Threats Post Covid-19

Covid-19 has accelerated changes in the working culture in all types of sectors. Pre Covid-19, Most of the employees were working from offices, which is a physically secure network, as well as their laptops or desktops, are adequately secured. Enterprise protection technologies secure employee systems from any type of cyber attack. Post Covid-19, only the staff who need direct access to the system or hardware is working from the office, the rest of the workforce has to operate from the less secured or vulnerable network.

Also due to this sudden shift and advancement in technology most challenging job is to keep the system secure. Hackers are targeting the technologies which expose vulnerable software or flaws in configuration or obsolete software. These are the soft targets for cybercriminals.

According to a report published by McAfee in November 2020, a 91% increase in threat is detected in the science and technology sector, Cyberattacks has increased by 602% in Quarter2. Attacks on cloud services reached nearly 7.5 million. The publicly disclosed security incident rose by 22% in Quarter2 out of which 35% attacks were Malware led. Account hijacking and targeted attacks are increased up to 17% and 9% respectively. Mobile malware increased by 15%. [1]

Cybersecurity threats Post Covid-19 are discussed below;

1) Account Take Over (ATO) attacks.

   The pandemic situation has created an opportunity for cybercriminals to accelerate innovation and developing new attacking tools. They are monitoring the usage pattern of the public, due to social distancing and restrictions laid by government agencies use of online retail, food delivery, and online education is increased. This resulted in a surge in the traffic of users which presented the opportunity to the cybercriminals to attack inexperienced users.

   In Covid-19 cybercriminals have increased the 'sophisticated' attacks using headless browsing tactics (without GUI) and Javascript enabled bots. [12] Even Cyber Criminals have developed advanced bots with detailed business logic capabilities that can crawl multiple pages and solve the CAPTCHA. In ATO attacks Cybercriminals obtain stolen credentials, on the dark web and public internet billions of compromised account credentials are traded. After testing these credentials credential stuffing tactics are used in launching manual or automated attacks with

ISSN: 2233-7857 IJFGCN

bots. Once the attacker has identified a valid credential, they can sell the account or use it for fraudulent activity.

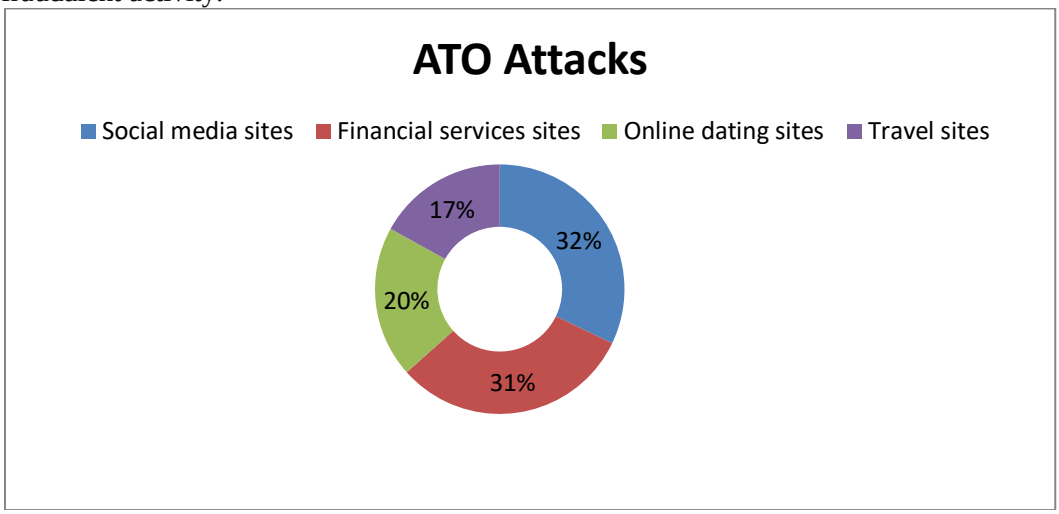

Figure 3: Statistics of ATO attacks on different sectors; [13]

2) Distributed botnets (DDoS Attack)

A botnet is a network of interconnected compromised devices, which are running single or multiple bots. In Coivid-19 situation cybercriminals has infected multiple devices with malicious bots to gather the quality IP address from a large range of residential addresses.

Using the command and control servers Botmaster controls the botnet remotely. For communication with other Botnet servers, Botnet masters create a P2P network.

DDoS attacked launched using any botnet are controlled by multiple masters sometimes working in a coordinated manner. Botnet on hire is also available as botnet rental services are auctioned and traded by using ambiguous service name of stressers or boosters.[14]

3) Megacart Attack or Virtual Skimming Attack

Megacart attack has grown by 20% in Covid-19 Pandemic. Due to the pandemic situation, many businesses are making quick changes and shifting to new online sites. These websites are a more vulnerable and soft target for attackers. Attackers are injecting malicious Javascript into online checkout software systems to steal personal finance data, email passwords, credit card information. In some Megacart, attacks users are redirected to lookalike domain names to capture the payment. In some attacks, the attacker snoops the data from the payment information form of the legitimate website by injection script on the payment page.

4) Ransomware

Ransomware belongs to the malware family, which is used to limit the user from accessing their system by encrypting files on users' systems till a ransom is paid. [15] Ransomware uses the same technique as other types of malware to infect the user system. Ransomware has a unique nature, which can be seen through its behavior and permanent effect on the user system. [16] Cyber Criminals are targeting Government related organizations and businesses, hospitals and health care centers, Educational Institutes, and Manufacturing Industry. Cybercriminals have also started to offer Ransomware-as-a-service on the dark web. [16]

During the Pandemic situation taking advantage of the panic situation, cybercriminals created fake health surveys targeting staff of the University of British Columbia (UBC). Corona Virus one of the new ransomware was spread through a fake Wise Cleaner site, promoting it as a system optimization tool. This ransomware contains two files; Corona Virus ransomware and password-stealing Trojan. Another attack was presumed to be caused by ransomware in the Czech Republic Covid-19 testing center at Brno, Which delayed the Covid-19 test result.

5) Mobile Threats

ISSN: 2233-7857 IJFGCN

New ransomware 'CovidLock' locks the victim's phone and asks to pay US$100 in bitcoin to regain access within 48 hours. Threats included in this ransomware are wiping out the phone data and publishing it on social media. According to Lukas Stefanko, the malware researcher at ESET, New ransomware detected named CryCrypto, posing as a contact tracing app for Canada's healthcare agency, health Canada. [17]

Android Trojans are used to gain access to a user's funds, requesting the user to log on to the fake banking screen and also steal the two-factor authentication codes. Cybercriminals developed fake websites to impersonate different apps like Covid-19 tracker, Government Coivd-19 awareness apps, financial loss compensation app, and video conferencing app. Android ransomware mostly does not lock the phone, but encrypt the data stored on external storage.[17]

6) Browser apps

New type of Cyberattack found in a pandemic situation is the Browser Apps. This attack is carried out by hacking routers' Domain Name System (DNS) settings to prompt the popup on web browsers. Victims have noticed that their web browsers are open on its own and display popup message prompting to download 'Covid-19 Inform App'. This app is wrapped with Oski info stealer, which will get installed on the device. Cybercriminals can steal browser cookies, history, saved information like login details, and financial information. [10]

7) Malicious Social Media Messaging (Mobile phishing)

According to the Lookout researchers report, in the last quarter of 2019 & the first quarter of 2020, a 37% surge is seen in a mobile phishing attack, which was centered on Covid-19. Cybercriminals know due to pandemic situations and lockdown constraints peoples are spending more time on the phone, either learning more information about Covid-19. Cybercriminals are taking the advantage of work from home facilities given by heavily regulated industry because of the sensitivity of data and high-value resources, as one mistake by an employee could make the whole network vulnerable.[9]

Cybercriminals created phish websites of Scotiabank or Royal Bank and blasted out messages using Canadian number asking the recipients to enter their account details. The only way to identify the fake page is the URL, but it can tweak by using a short URL. The mobile device has a small screen and limited ability to carefully check links and attachments before clicking on them. Even after Covid-19, many companies are planning to work from home for their employees, proactive defense against a phishing attack is going to be difficult.

IV. Security Challenges and Measures Post Covid-19

Covid-19 pandemic is expected to be temporary, with an expected time horizon of weeks or months. This situation has forced industry & individuals to follow new practices such as social distancing, remote working, online lectures in schools & colleges, etc. Because of the pandemic, a person has realized that life cannot come to standstill, people have realized that within a short period anything could be done remotely via computer or Smartphone. This situation has given a rise to cybersecurity challenges because while peoples are focused on safety measures, cybercriminals are capitalized to launch a well-planned attack.

People have to take preventions and precautions to safeguard from attacks;

- Peoples should keep their information safe, take the backup of all the files regularly, and store it independently on external drives or cloud. Always verify the URL for a legitimate website before entering login credentials or sensitive information. Download mobile applications or any other software only from trusted platforms.
- Talk with family members about precautions to be taken while surfing. Social media account privacy settings need to be check and updated on regular basis. Change your password often and ensure that passwords are complex. Do not click on any short URL, hyperlink or attachment received via social media apps or messaging services, or emails, which you are not expecting.

ISSN: 2233-7857 IJFGCN

Organizations have to take precaution to overcome these challenges:

- Cybercriminals are making use of new technologies such as Artificial Intelligence and Machine Learning to launch sophisticated attacks. The cybersecurity team needs to reset their security system to ensure there are no digital holes in the fence. They need to understand the new age cyber risks and prepare the defense for the same.
- Peoples are now demanding access to any application from any available device. The cybersecurity team has to design & deploy new next-generation identity and access control mechanisms to provide an effective cybersecurity posture for an organization.
- The main risk of work from home policy is bring-your-own-device (BYOD). This policy needs to be updated, as users are using their systems that are less secured from home which is having less secured network infrastructure. The cybersecurity team needs to prepare a comprehensive checklist for new systems & BYOD systems with strict VPN policies.
- The use of BOYD systems is increased due to a remote working situation in the pandemic. These devices are typically used from the less secure home networks. To ensure the safety of critical business data, the cybersecurity team needs to implement multifactor authentication for accessing such information with the capability to store critical data with strong encryption technique.
- The organization needs to implement zero-trust policies, which states that no one is trusted by default, verification is required for every user who is trying to gain the access to resources on the network. This added layer of security is useful for avoiding data breach incidents.
- Threat detection and response capabilities must include advanced technologies like Artificial Intelligence, Machine Learning, and Big Data. These can be used to detect adverse behavior of the machine speed, without human interventions.
- Taking into account the risk posses from work from home and the increase in cyber attacks adequate investment in cyber insurance is a need. Even if any security parameter is breached cyber insurance can protect the business from the high financial implications of such failure.

V. Conclusion

Due to the Covid-19 pandemic situation and lockdown situation world is shifting to the digital era, where people are avoiding face-to-face meetings and shifting towards virtual face-to-face meetings using video conferencing app. Peoples and organizations are preferring work from home as they have seen growth in work efficiency. The use of e-commerce websites and apps increased which is creating ample opportunity for cybercriminals to launch sophisticated attacks in interest of financial gain or other interest. Cybercriminals are not only targeting the organization, now they have started to target Government apps, health care systems as well as individuals. This paper has analyzed the attacks carried out by the cybercriminals during the Covid-19 and presented the attacks which will be vital Post Covid-19. These cybersecurity threats have given rise to new challenges, and cybersecurity professionals will be a crucial role to protect their organizations' people, technology data from the new risks of more sophisticated cybercriminals.

References:

1. https://www.thehindubusinessline.com/news/covid-19-related-cyber-attacks-soar-in-q2-of-2020-report/article33028076.ece [Accessed: 26-Dec-2020].
2. Khan, Navid & Brohi, Sarfraz & Zaman, Noor. (2020). Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic. 10.36227/techrxiv.12278792.v1.
3. https://www.businesswire.com/news/home/20200507005631/en/COVID-19-Outbreak-Video-Conferencing-Demand-Rises-due-to-Social-Distancing---ResearchAndMarkets.com [Accessed: 26-Dec-2020].
4. https://www.techrepublic.com/article/who-has-banned-zoom-google-nasa-and-more/ [Accessed: 26-Dec-2020].
5. https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/ [Accessed: 26-Dec-2020].

ISSN: 2233-7857 IJFGCN

6. https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/ [Accessed: 26-Dec-2020].
7. https://www.gartner.com/en/newsroom/press-releases/2020-04-24-gartner-says-52-percent-of-legal-and-compliance-leaders-are-concerned-about-third-party-cybersecurity-risk-rince-covid-19 [Accessed: 25-Jan-2021].
8. https://www.prnewswire.com/in/news-releases/covid-19-pandemic-sparks-72-ransomware-growth-mobile-vulnerabilities-grow-50--817268901.html. [Accessed: 25-Jan-2021].
9. https://www.techrepublic.com/article/covid-19-emergence-leads-to-37-jump-in-mobile-phishing-attacks-in-2020/ [Accessed: 25-Jan-2021].
10. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains [Accessed: 25-Jan-2021].
11. https://www.pandasecurity.com/en/mediacenter/news/covid-cybersecurity-statistics/#country [Accessed: 26-Dec-2020].
12. https://www.scmagazine.com/home/opinion/executive-insight/5-ways-web-attacks-will-change-post-covid/ [Accessed: 25-Jan-2021].
13. https://www.helpnetsecurity.com/2020/10/06/ato-attacks-surge/ [Accessed: 25-Jan-2021].
14. https://www.imperva.com/learn/ddos/botnet-ddos/ [Accessed: 25-Jan-2021].
15. https://www.trendmicro.com/vinfo/in/security/definition/ransomware#:~:text=What%20is%20Ransomware%3F,unless%20a%20ransom%20is%20paid. [Accessed: 25-Jan-2021].
16. Salah, Mohammed & Marhusin, M.F. & Sulaiman, Rossilawati. (2018). A Two-stage Malware Detection Architecture Inspired by Human Immune System. 1-4. 10.1109/CR.2018.8626867.
17. https://www.welivesecurity.com/2020/07/15/mobile-security-threats-covid19-beyond-qa-lukas-stefanko/ [Accessed: 25-Jan-2021].
18. Tilak, G., & Bhaumik, A. A Review on Security and Usability of Graphical User Interface Design.

ISSN: 2233-7857 IJFGCN