iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** X **Month of publication:** October 2020

DOI: https://doi.org/10.22214/ijraset.2020.32013

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue X Oct 2020- Available at www.ijraset.com

Cyber Threats and Attack Vectors during COVID-19

Girshel Chokhonelidze[1], Giorgi Basilaia[2], Mikheil Kantaria[3]
[1, 2, 3]*Business and Technology University*

Abstract: ***The ongoing world pandemic caused by COVID19 has had a significant impact on cyber incidents and has led to a sharp increase in cybercrime activity.***
The shift of a large proportion of users to remote work has increased their use of ICT systems. The inadequate observance of cyber-hygiene norms and low awareness has turned large parts of users into vulnerable groups, and the cybercriminals benefited from it. Cybercriminals started phishing campaigns using social engineering and COVID19 related issues. They have created fake online resources and content with the aim to infect users and spread malware.
During the pandemic, phishing attacks increased significantly and became dominant.
Cybercriminals use e-mail as the main source of malware, they also actively create fake online resources and applications that are as close as possible to real sought-after and up-to-date content.
Not only the activity of cybercriminals for financial gain was revealed as one of the motives of cyber-attacks, but political purposes play a big part in it also. The number of attacks increased in all sectors, including governments, industry, healthcare, service providers, critical infrastructure, and consumers.
The current trend in cyber-attacks has highlighted the importance of cybersecurity in modern challenges and business processes, across all areas. The level of user awareness and adherence to proper rules of cyber hygiene was manifested as an important and critical link. Because only at the technical level, even in the presence of cybersecurity controls, the user is a vulnerable and important group in the whole security chain.
Keywords: Cyberthreats, Attack vectors during Covid-19, Cybersecurity, ICT Systems

I. INTRODUCTION

Due to the ongoing digital transformation in the world, cybersecurity and related issues have been a challenge for many years for the whole world, both for the public and private sectors. Cyber-attacks are being refined day by day, and they are becoming more diverse and the number of cyber incidents is growing rapidly.
The ongoing Covid19 pandemic has had a significant impact on cyberspace as well.
During the Covid19 pandemic, not only financial but also political motives emerged as the motive for cybercriminals. The number of attacks has increased in all sectors including governments, industry, healthcare, service providers, critical infrastructure, and consumers. [1]
According to the mid-year report of 2020 of the leading Company in cybersecurity "Checkpoint", "COVID-19 related phishing and malware attacks increased dramatically from under 5,000 thousand per week in February to over 200,000 per week in late April. Also, in May and June, as countries started to ease lockdowns, threat actors stepped up their non-COVID-19 related exploits, resulting in a 34% increase in all types of cyber-attacks globally at the end of June compared to March and April" [2]
The number of cyberattacks on various organizations and agencies in the healthcare sector has increased significantly. For example, the World Health Organization (WHO) has reported a 500% increase in cyber-attacks against it since the onset of the Covid19 pandemic. [3]
According to the Interpol report, phishing, SCAM and various types of online frauds amount a significant share of cyber threats, with the percentage of 59%, followed by malware (Remote Access Trojan, info stealers, spyware, banking Trojans) and ransomware - 36%. It has also been revealed that cybercriminals register fake domains and create fake online resources with Covid 19 related content and keywords to mislead users and infect their systems or to obtain various types of sensitive information. Malicious domain registration increased by 569% from February to March. One example of the creation of fake resources is the Coronavirus Spread Map, which closely resembled the valid map created by Johns Hopkins University, which was very popular around the world and is the global platform for Covid19 statistics.[4]
This fake domain, in case of a visit, infected the system in various ways and allowed the attacker to gain unauthorized access or to steal sensitive information [5]
Also, cybercriminals created a windows application that also infected the target system and gave access to the attacker. Cybercriminals used previously known malware - Azorult Trojan - to infect the system.[6],[7]

Fig. 1 Fake coronavirus map

This threat ranks third with 22%. Fake news related to Covid19 is in fourth place with 14%. Cybercriminals try to mislead individuals by spreading various false information, sowing panic, spreading conspiracy theories, etc. “First, the six major themes of fake news are health, religious-political, political, crime, entertainment, religious, and miscellaneous.” Health-related fake news (67.2%) dominates the others. [8]

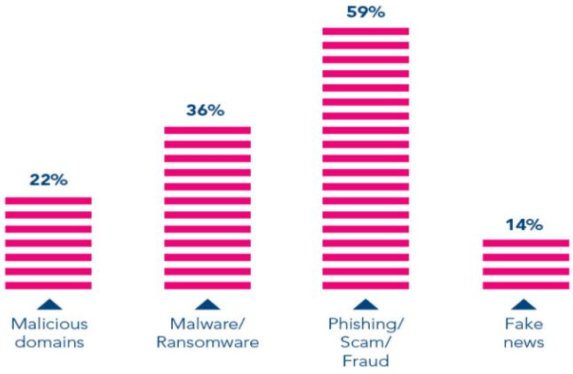


Fig. 2 Distribution of the key COVID-19 inflicted cyber threats based on member countries’ feedback

According to the 2019 mid-year report of one of the leading companies in the cybersecurity field, “Checkpoint”, due to the current world trends, the attack vectors related to mobile devices held first place in the cyberattack categories, which moved to second place in 2020 and crypto miners took the first place, the percentage of botnets, Banking malware and ransomware has increased. [9], [10]

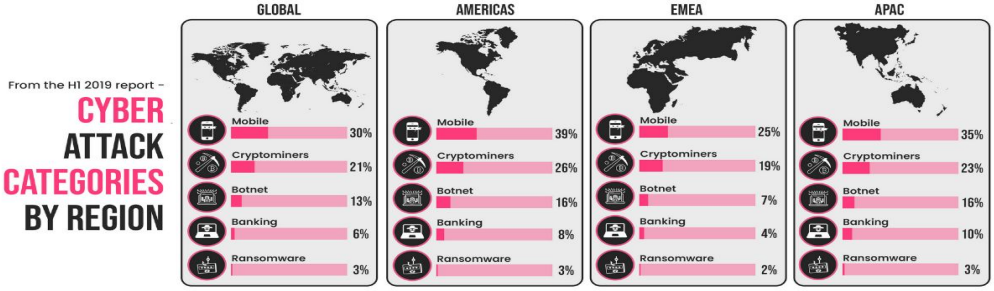


Fig. 3 2019 H1 Report by Checkpoint

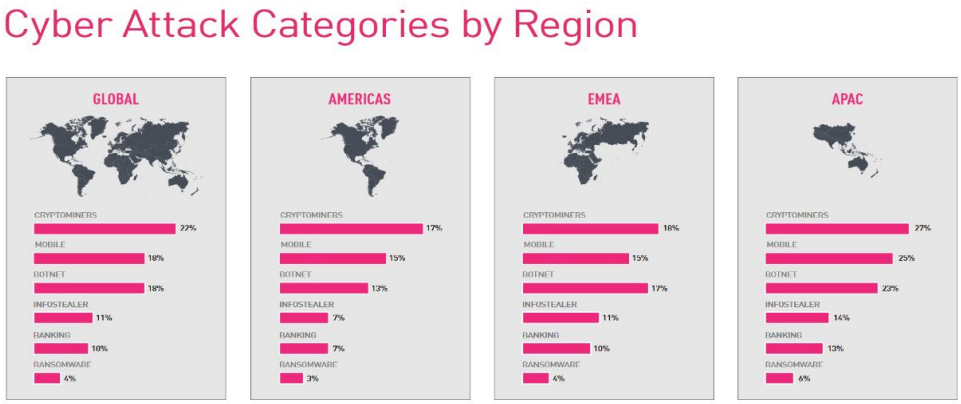


Fig. 4 2020 H1 Report by Checkpoint

Cybercriminals mostly use WEB and Email protocols to infect systems. Through these services, various types of malicious code files enter the system. Based on a "Checkpoint" study, the dominant malicious file types were identified, where the .exe extension files used in Microsoft operating systems are dominating. Also, Microsoft Office and PDF extension files. As the analysis shows, the targets of cybercriminals are mostly Microsoft systems. [10]

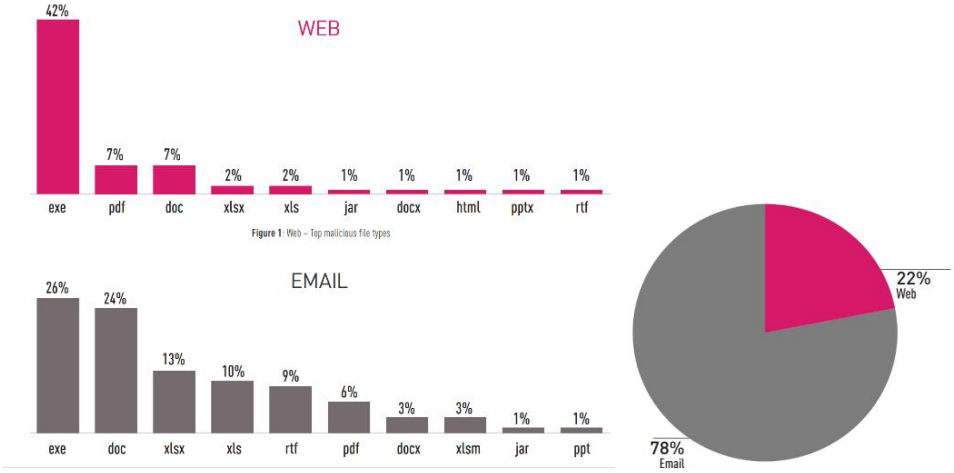


Fig. 5 Top Malicious File types - Web vs. Email

Of these sources of infection, Email stands out significantly, accounting for almost 80% of infections compared to the WEB. . [10] Using email, cybercriminals have become more active in almost all sectors and have launched widespread Phishing campaigns on COVID19-related topics. Email has become a major attack vector against individuals and organizations. [1]

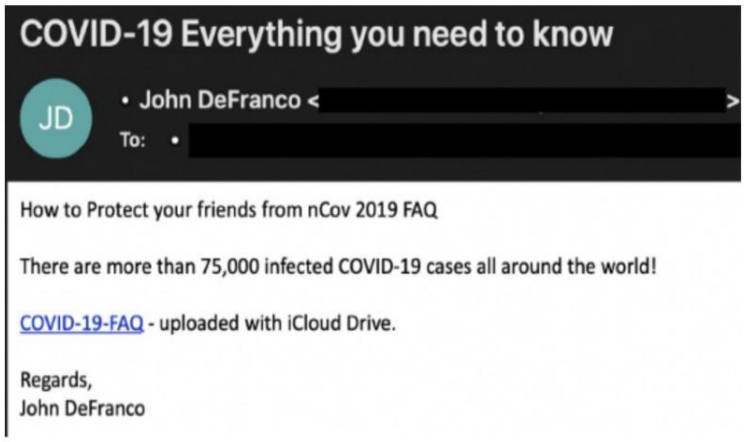


Fig. 6 Example of a COVID-19 phishing email from FireEye's Report

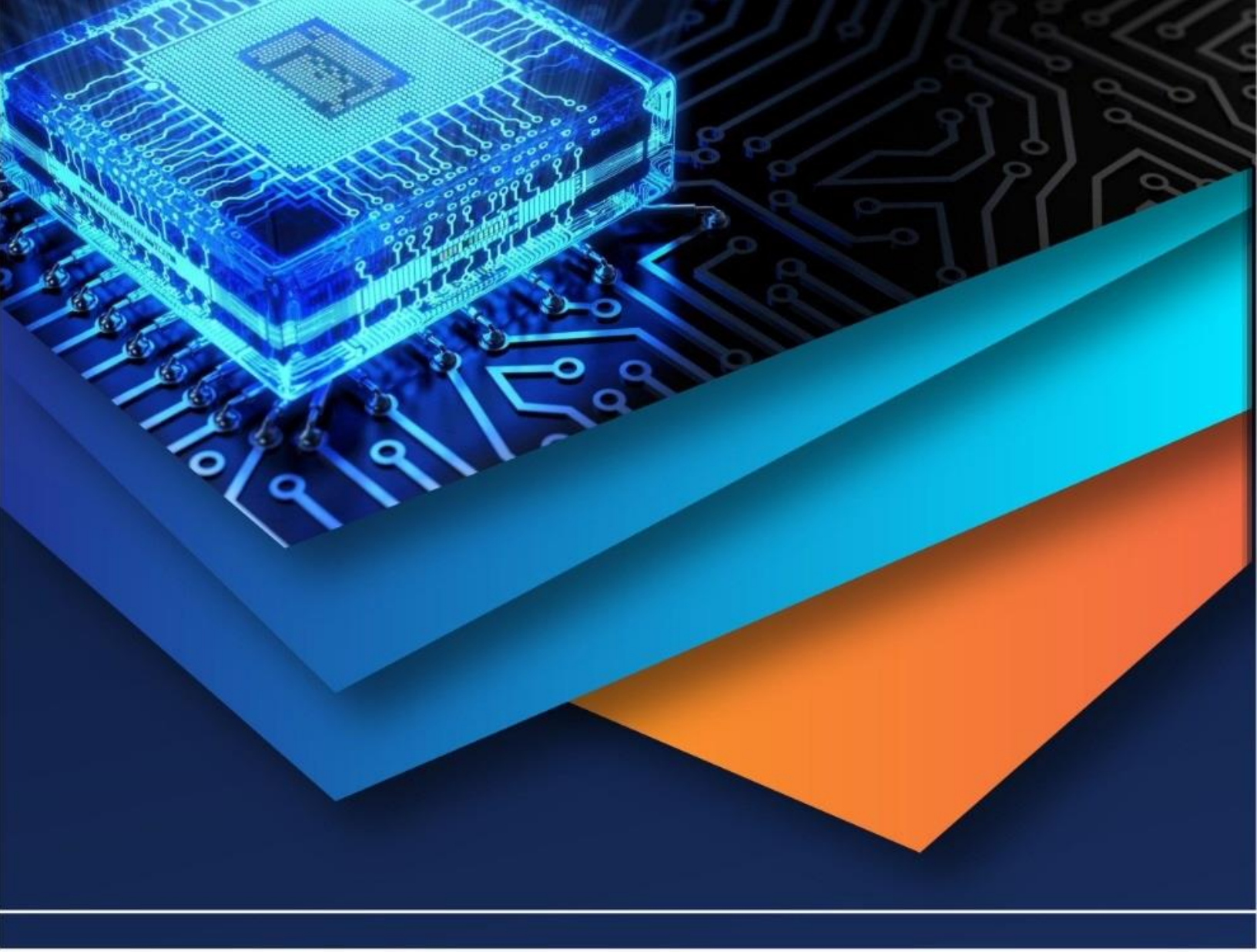
As a large number of studies and statistics show, Covid19 has significantly increased the activity of cybercriminals. Due to the pandemic, a large proportion of employees have moved to remote work worldwide, which has increased the intensity of use of various communication systems and made users somewhat more vulnerable to cyber threats. With all this in mind, cybercriminals have focused on social engineering, which aims to mislead and infect users by using improper cyber-hygiene and low awareness. Using appropriate social engineering, emails are an effective method of infecting victims. Even if the organization and information systems have proper technical controls in place to ensure cyber and information security, users will remain unsafe and vulnerable if they do not have the appropriate awareness of information security and do not comply with cyber hygiene norms. By misleading users, the attacker bypasses security technical controls and successfully manages to compromise the system or obtain sensitive information. Such an incident poses a critical threat not only to individuals but to the entire organization or IT infrastructure.

II. CONCLUSIONS

Systematic awareness-raising campaigns are needed to ensure the appropriate level of awareness for the employees of the organization as well as a systematic, active control of their awareness and observance of cyber hygiene norms. The trend of ongoing cyber incidents and the growing reliance on technology have highlighted the importance and role of cybersecurity in everyday life, which requires a proper dynamic approach and the creation of an appropriate control environment, both in organizations and in an individual's devices and information systems.

REFERENCES

[1] Check Point Press Releases. (2020) [Online]. Available: https://www.checkpoint.com/press/2020/check-point-research-covid-19-pandemic-drives-criminal-and-political-cyber-attacks-across-networks-cloud-and-mobile-in-h1-2020/
[2] Check Point Software Technologies Ltd, "Check Point Research: COVID-19 Pandemic Drives Criminal and Political Cyber-Attacks Across Networks, Cloud and Mobile in H1 2020." [Online]. Available: https://www.globenewswire.com/news-release/2020/07/22/2065610/0/en/Check-Point-Research-COVID-19-Pandemic-Drives-Criminal-and-Political-Cyber-attacks-Across-Networks-Cloud-and-Mobile-in-H1-2020.html. [Accessed: 28-Oct-2020].
[3] WHO (2020) [Online]. Available: https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance
[4] INTERPOL, "INTERPOL report shows alarming rate of cyberattacks during COVID-19," *Interpol*, 2020. [Online]. Available: https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19. [Accessed: 28-Oct-2020].
[5] F. Mouton, "COVID-19 : Impact on the Cyber Security Threat Landscape," no. March, 2020.
[6] "Fake Coronavirus Map Delivers AZORult malware | Information Security at UVA, U.Va." [Online]. Available: https://security.virginia.edu/fake-coronavirus-map. [Accessed: 28-Oct-2020].
[7] Reason Labs. (March 9, 2020). COVID-19, Info Stealer & the Map of Threats – Threat Analysis Report. Reasonsecurity.com. Accessed 10 October 2020
[8] M. Al-Zaman, "COVID-19-related Fake News in Social Media," *medRxiv*, p. 2020.07.06.20147066, Jul. 2020, doi: 10.1101/2020.07.06.20147066.
[9] Check Point Software Technologies Ltd, "Cyber-attack categories by region H1 2019." [Online]. Available https://research.checkpoint.com/2019/cyber-attack-trends-2019-mid-year-report/ [Accessed: 28-Oct-2020].
[10] Check Point Software Technologies Ltd, "Check Point Research: Cyber-attack categories by region H1 2020." [Online]. https://research.checkpoint.com/2020/cyber-attack-trends-2020-mid-year-report// [Accessed: 28-Oct-2020].
[11] "With COVID-19 Themed Campaigns on the Rise, Here's How to Manage Email Phishing Risks | FireEye Inc." [Online]. Available: https://www.fireeye.com/blog/executive-perspective/2020/03/managing-email-phishing-risks.html. [Accessed: 28-Oct-2020].



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY