The Impact of COVID-19 on Cybercrime and Cyberthreats

Iulian Coman
Ioan-Cosmin Mihai
European Union Agency for Law Enforcement Training[1]

Abstract:
The paper describes the evolution of cyber-attacks, based on different official reports from law enforcement agencies and cybersecurity companies. It focuses on the EMPACT priority 'cybercrime-attacks on information systems' and analyses the main types of malware (banking trojans, ransomware, cryptojacking and botnets malware) and their evolution during the COVID-19 Pandemic. The paper presents both online threats vectors (email-based attacks, web-based attacks, social media scams) and offline threats and their impact to the information systems. Disruptive technologies like artificial intelligence, quantum computing, 5G technology, Internet of Things (IoT) and social networks presents a lot of advantages, but also can be used by bad actors against us. The present article underlines the importance of education and training in this field and recommends measures to fight with the cybercrime phenomenon.

Keywords: cybercrime, cyber threats, cyber-attacks, social-media, COVID-19 patterns

Introduction

The measures taken by national governments starting with March 2020, increased the use of digital applications by more than 10 percent, and together with this the insecurity of the population. Coronavirus had made a clear path for cybercriminals, that through use of social media and messaging platforms gained easy access to potential victims with a significant increase in activity related to child sexual abuse and exploitation and medical related scams. According to Facebook's Government Requests for User Data, the social media platform (includes Instagram) saw more than 150,000 total law enforcement agency requests in the European Union in 2020 (first six months) — with over 40.000 requests more than in 2019. In the same period of 2020, Europol received from the National Center for Missing and Exploited Children and increasing number of referrals, compared with the same period in 2019.

The online distribution of counterfeit pharmaceutical and sanitary products, including coronavirus related test and vaccines, has been also demonstrated as a criminal opportunism during the COVID-19 pandemic. In August 2020, European customs agencies inter-

1 Authors' emails: iulian.coman@cepol.europa.eu, ioan-cosmin.mihai@cepol.europa.eu

cepted more than 8.5 million masks without CE certification.

According to the latest statistics, the COVID-19 Pandemic has hastened the digital transformation process, with numerous services moving to the internet. The new technology offers many benefits, but it also poses certain hazards, as present flaws might be exploited by cybercriminals. The frequency of cyber-incidents and cyber-attacks has recently surged dramatically due to a lack of Cyber security awareness and training.

Cybercrime is currently taking advantage of people's insecurity and demand for information. The prevalence of security incidents in recent years has substantiated the continuous escalation of vulnerability exploitation within the virtual information environment, predominantly by organized groups and state actors. The complexity of cyber-attacks has also developed at an alarming rate, culminating with some being publicized as global epidemics due to their impact and spread momentum. Boosting the preparedness and advocating for a proactive approach in the design and creation stages of digital infrastructure are the key efforts for making cyber space a safe place for everyone.

The predominant types of cyber-attacks deployed today are carried out through malware applications, denial of service (DoS, DDoS), by disrupting and exploiting electronic mail and web applications, the last category being represented by APT attacks (Advanced Persistent Threats).

The data from the most used social media platforms indicate an increase in users over three year time, increasing year by year, because the access to internet and smart devices that people gain each year and an increase caused by the Pandemic.

Eurofund suggests that close to 40% of people working in EU, converted in full telework in 2020[2]. Having more than 80 percent of people worldwide encouraged to work remotely, further on, having as most increased cybercrimes on socials media phishing attacks, malware sent via chats, social media scams and child sexual abuse materials. Social engineering and phishing changed and evolved, having users thirst for information mainly on the subject of COVID-19.

Types of criminal acts

Malware attacks

As reported by the European Union Agency for Cybersecurity (ENISA) in their most recent report, this is the most widespread type of cyber-attack. Malware, or malicious software, is any malicious code or program that is harmful to a computer system. These pieces of malicious code can be viruses, trojans, worms, and, based on their scope, ransomware, spyware, rogueware or scareware (ENISA, 2020).

According to ENISA, there are more than 230.000 new strains of malware released on internet every day. In addition, there is a 50% increase in malware designed to steal personal data and a 265% increase in file-less malware (ENISA, 2020). Traditional malware was inserted in files, so the users could infect their computer systems when they downloaded these infected files from websites or emails. Nowadays, the cybercriminals use malicious scripts that can compromise the targets when the users access the compromised websites and they do not have properly configured cybersecurity tools.

During the pandemic time, there was an increase of the malware designed for mobile devices. Most of the users do not protect enough their mobile devices, so the cybercriminals can easily compromise them in order to steal personal data or online banking credentials.

2 EUROFUND Report on Living, working and Covid-19, 28 September 2020

Figure 1: ENISA Top Threats 2019-2020

Top Threats 2019-2020		Assessed Trends	Change in Ranking
1	Malware	---	---
2	Web-based Attacks	---	↗
3	Phishing	↗	↗
4	Web application attacks	---	↙
5	Spam	↙	↗
6	Denial of service	↙	↙
7	Identity theft	↗	↗
8	Data breaches	---	---
9	Insider threat	↗	---
10	Botnets	↙	↙
11	Physical manipulation, damage, theft and loss	---	↙
12	Information leakage	↗	↙
13	Ransomware	↗	↗
14	Cyberespionage	↙	↗
15	Crytojacking	↙	↙

Computer viruses are applications with varying destructive capabilities, developed to infect one or more computer systems. *Viruses* have two main features: they attach to harmless software and self-multiply in the infected system. *Trojans* are software that obfuscate their true nature through legitimate operations, but in actuality, they attempt to expose system and application vulnerabilities and to open ports in the operating system, to provide attackers with an avenue of remote access. *Computer worms* are applications with destructive effects, which infect the computer system and then propagate through the Internet. (Mihai et al., 2018) Worms are designed to search for systems with vulnerabilities, infect them and perform harmful operations, and then try to proliferate further.

Adware is a class of software that, once installed on a system, aggressively displays ads to the user. *Spyware* is software that covertly captures various information about the user's activity, such as keystrokes, screenshots of their running applications or private details on their Internet usage. *Ransomware* is a type of malware that restricts access to the computer's data by encrypting files, and prompts the user to make a payment in order to remove the encryption. Some types of ransomware encrypt data on the system's hard drive, as well as any files it can access over the local network and in Cloud storage, to affect backups, while others may simply block the computer system and display messages to coerce the user into paying the ransom.

Rogueware are applications that mislead users about false infections detected in their operating system and request payment in order to remove them. Most often, these claim to remove malware found on computers, but in fact install additional software with increasingly detrimental effects. *Scareware* is software that induces anxiety and fear in users for the purpose of marketing fake applications. (Mihai et al., 2015)

Denial of service attacks

Compromising the operation of certain internet services is the explicit, intended consequence of a Denial of Service (DoS/DDoS) attack. One of the most common DDoS attacks is a packet flood, through which a disproportionate number of Internet packets are sent to the victim's system with the goal of blocking all available connections and slowing network traffic to a crawl, leading to a complete halt of the services provided by the attacked system.

Email attacks

Attacks that make use of or target email have increased exponentially lately. Based on the cyber criminals' ultimate purpose, email attacks can belong to one of several categories. *Email bombing* consists of sending a significant number of emails with large attachments to a specific email address. This leads to the exhaustion of free space on the server, making that email account inaccessible. (SRI, 2021) *Email spoofing* is the practice of sending emails with a modified, most often fake

sender's address, in order to hide the real identity of the sender and potentially extract confidential details or the data needed to access an account. *Spamming* is an attack comprised solely of sending unsolicited emails with commercial content. The purpose of these emails is to trick their recipients into accessing disreputable sites and buying services or products of a dubious nature. *Email phishing* is a rapidly-expanding attack type, in which specifically-crafted messages are sent to determine recipients to provide bank account information, credit card details, passwords, or other private data, (ENISA, 2020) or to make a payment seemingly on behalf of someone known to the victim.

Web application attacks

Attacks targeting Web applications are experiencing rapid growth, propelled by the explosive development of Web technologies that support and enhance the design of highly interactive, dynamic content platforms, with consistent user interaction. Such platforms inevitably contain vulnerabilities that can be leveraged by cybercriminals to bypass security measures and gain unauthorized access to user data. (ENISA, 2020) The most common forms of this attack are:

SQLi: SQL injection (Structured Query Language) is the practice of altering an SQL query that is transmitted to the database by inserting data, which changes the logic and purpose of the query. This enables the attacker to avoid authentication mechanisms.

XSS (Cross-Site Scripting) allows an attacker to modify or insert scripts into a site, which are then executed in the victim's browser when they access the infected site.

Cross-Site Request Forgery (CSRF): a malicious actor exploits an established trust relationship between authenticated users and a web application. Thus, they gain control over the victim's session, allowing them to impersonate a legitimate user and perform any action within their context.

Man in the Middle: Cyber criminals intercept communications between users and websites in order to retrieve unencrypted credentials.

Advanced Persistent Threats

Advanced Persistent Threats represent complex cyber-attacks performed over an extended period of time, aimed at a particular target, with a number of objectives, such as compromising the system, extracting information on / from the victim or, occasionally, planting misleading information. Targets can be governments, military installations, corporations, or even individuals. (Mihai et al., 2018) An APT is typically comprised of several complementary cyber-attacks. Generally, such an operation encompasses collecting data on the target, identifying a potential exploit and pursuing it, infecting the target and leveraging any extracted information, in accordance with the overarching scope. Conventionally, only terrorist organizations or nation states possess the technological capability and the requisite financial resources to manifest such elaborate cyber-attacks.

Child Sexual Abuse Material

During the pandemic, most of the schools converted into online learning. Non-stop access to internet, to social media platforms and messenger applications, have raised the danger for potential victims. During the 2020 pandemic start and governments' imposed lockdowns, more that 168 million children had to stay home because of the closed schools, says UNICEF United Nations Children's Emergency Fund[3].

Based on the available data[4] from the European Agency for Law Enforcement Cooperation (Europol), an increased level of activity for distribution of CSAM has been identified between March and April 2020 (Fig. 2). The activity range from children who are being forced by criminals to produce material, or offenders that gain access through social media or messenger platforms using phishing methods. (Europol, 2020)

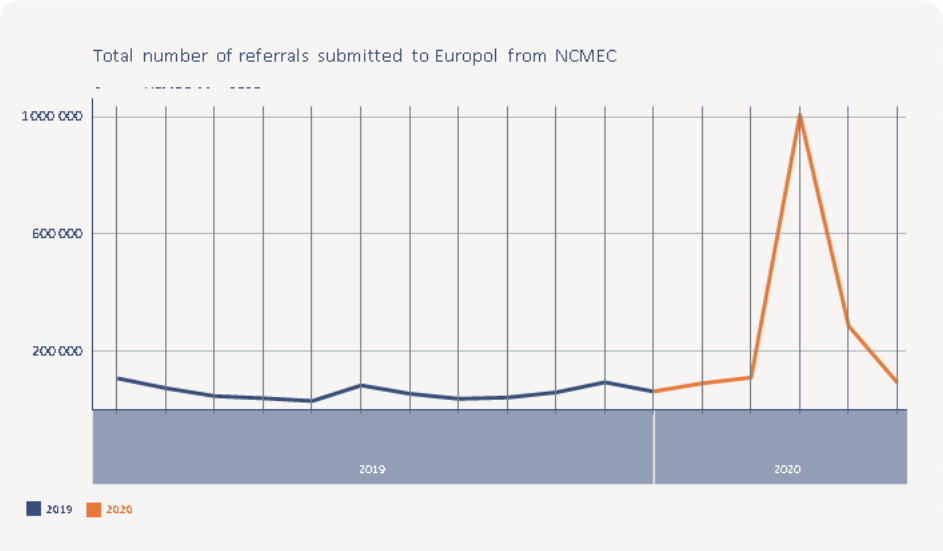
During the pandemic the modus operandi of cybercriminals in connection with CSAM, particularly happened via P2P network sharing, one to one distribution and mass sharing on social media platforms, using fake social media accounts, encryption (TOR, VPN), in the end materials ending up on dark web (Europol, 2020). Data from NCMEC, the National Center for Missing and Exploited Children, and Europol indicated 106% increase of this type of activity.[5]

3 https://www.unicef.org/press-releases/schools-more-168-million-children-globally-have-been-completely-closed

4 EUROPOL Report on Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic, June 2020

5 Europol report, Catching the virus- cybercrime, disinformation and the Covid-19 pandemic, 3 April 2020

Figure 2: NCMEC, May 2020



Another type of cyber-harassment that increased in 2020 was zoom bombing, when unwanted users gate-crash video meetings with malicious purposes, including sharing pornographic or hate images. (Interpol, 2020)

Regarding law enforcement training needs, based on the report[6] released by CEPOL, the European Agency for Law Enforcement Training, OSINT tools, methods of investigations, dark web as well as prevention and cooperation should be tackled further on by law enforcement training needs. (CEPOL, 2020)

Medical scams

Covid-19 related scams witness three waves of development, starting with the first and second wave related to cures, prevention and fake testing kits and finishing with fake pharmaceutical treatments. (Council of Europe, 2020)

The study[7] published by the Journal of Medical Internet Research Public Health and Surveillance, mentions that over 6 mil tweets and over 200.00 Instagram posts with suspect marketing sale of covid 19- health products from March to May 2020. The posts included fake covid products for sale, fake testing kits, prevention cures, effective vaccine or therapeutic treatments. (Tim et al., 2020)

Cyberbullying

The European Commission defines cyberbullying as repeated verbal or psychological harassment carried out by an individual or a group against others through online services and mobile phones and based on the recent reports, hate between kids and teens during online classes increased with 70%, especially during Zoom or other videoconferencing platforms, but also on gaming platforms as Discord, or other popular social media applications.

Conclusion

The COVID-19 pandemic altered the lives of billions of people in the world and due to governments' lockdowns, new-normal changed the way of living and working and more and more attention was directed to the internet-based activities.

While greater usage of digital solutions has helped to reduce the chance of getting the virus while also allowing individuals to continue working and studying, it has also raised cybersecurity concerns. Simply said, the more people who use digital platforms, the higher the strain on existing cybersecurity systems, and the greater the risk of possible breaches. With the rate of proliferation and complexity of cyber-attacks at all-time highs, steps must be taken to deploy safeguards that can effectively block the vast majority of these attacks, as well as promote a safety-first mindset that increases public preparedness and reduces the attack

6 CEPOL report on Impact of COVID-19 on law enforcement operations and training needs, 1st of July 2020

7 Tim KM et al, Big Data, Natural Language Processing, and Deep Learning to Detect and Characterize Illicit COVID-19 Product Sales: Infoveillance Study on Twitter and Instagram, August 2020

surface of the human factor as an ever-present potential vulnerability.

In order to provide the opportune climate, implementing and maintaining proper cybersecurity regulations to equip the involved institutions with the means of preventing the escalation of ruthless attempts, and developing a cyber-defense culture, have to be done through active joint effort between public, private and research entities. Given the magnitude of the threat, many governments and corporations in emerging nations may lack the expertise and resources required to put in place sufficient measures. Law enforcement training, as a response to the COVID-19 pandemic patterns, should address new modi operandi in cyberspace and use of open source intelligence, in the long and short term. Law enforcement faces multiple challenges and due to lack of capacities in training and gaps in legislation and jurisdictional issues, further on investigative capacities being assigned to other crimes during the pandemic, delays of information exchange and lack of in-time identification of criminals increased.

We can conclude that cybercrime is already a viable career choice and continuous cooperation training would keep LE up-to-date and aware of the challenge. Cyber-attacks and crimes can only be reduced to an acceptable level by increasing education, prevention, and as well as digital literacy programs to be strengthened. Further on and law enforcement agencies' resources to prevent and investigate cybercrime must be bolstered through targeted recruitment of young personnel.

References

- CEPOL (2020) *Impact of COVID-19 on law enforcement operations and training needs*.
  Available from: https://www.cepol.europa.eu/sites/default/files/CEPOL_TNA_Domestic_Violence_Covid19.pdf
- Council of Europe (2020) *Cybercrime and COVID-19*.
  Available from: https://www.coe.int/en/web/cybercrime/-/cybercrime-and-covid-19.
- ENISA (2020) *ENISA Threat Landscape 2020 – Malware* (report).
  Available from: https://www.enisa.europa.eu/publications/malware/.
- ENISA (2020) *ENISA Threat Landscape 2020 – Phishing* (report).
  Available from: https://www.enisa.europa.eu/publications/phishing/.
- ENISA (2020) *ENISA Threat Landscape 2020 - Web application attacks* (report).
  Availabl from: https://www.enisa.europa.eu/publications/web-application-attacks/.
- ENISA (2020) *ENISA Threat Landscape 2020 – Spam* (report).
  Available from: https://www.enisa.europa.eu/publications/spam/.
- EUROFUND (2020) *Report on Living, working and Covid-19*.
  Available from: https://www.eurofound.europa.eu/sites/default/files/ef_publication/field_ef_document/ef20059en.pdf
- EUROPOL (2020) *Catching the virus-cybercrime, disinformation and the Covid-19 pandemic*.
  Available from: https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic
- EUROPOL (2020) *Report on Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic*.
  Available from: https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic
- Hutchins, E.M., Cloppert, M.J. & Amin, R.M. (2010) Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Lockheed Martin Corporation.
- INTERPOL (2020) Covid 19 – Child Sexual Exploitation and Abuse threats and trends.
- Mihai, I.C., Ciuchi, C., & Petrică, G. (2018) Current challenges in the field of cybersecurity - the impact and Romania's contribution to the field', Ed. Sitech.
  Available from: http://ier.gov.ro/wp-content/uploads/2018/10/SPOS_2017_Study_4_FINAL.pdf
- Mihai, I.C., Petrică, G., Ciuchi, C. & Giurea L. (2015) Cybersecurity challenges and strategies. Ed. Sitech.
- SRI (2021) Hybrid warfare and cyber-attacks. Intelligence Journal.
  Avaialble from: http://intelligence.sri.ro/razboi-hibrid-si-atacuri-cibernetice/.

- Tim, KM (2020) Big Data, Natural Language Processing, and Deep Learning to Detect and Characterize Illicit COVID-19 Product Sales: Infoveillance Study on Twitter and Instagram.
  Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7451110/
- UNICEF (2020) COVID-19: Schools for more than 168 million children globally have been completely closed for almost a full year.
  Available from: https://www.unicef.org/press-releases/schools-more-168-million-children-globally-have-been-completely-closed.