Journal
of Danubian
Studies
and Research

Cyber Attacks in the Context of the Pandemic Covid-19

Ionel Vladimir Vîrgolici[1], Alina Melania Ioniță[2], Alexandru Drăgănescu[3], Ionel Cătălin Stegăroiu[4]

Abstract: Information plays a crucial role in maintaining interpersonal relationships and developing society. The use of information technologies has caused a rapid change in our society. Although society bears the negative consequences of cybercrime, technology is still used in a wide variety of fields. This proves that it is, in fact, indispensable. To limit cybercrime, states should continue to develop computer technology and create legislation to criminalize harmful acts committed through technology. It is also necessary that the people involved in the fight against this phenomenon receive the necessary training. It is, at the same time, important that the population is well informed regarding the security of IT systems, thus providing an effective barrier against IT crime.

Keywords: cyber-attacks; COVID-19 virus; telework; security

1. Introductory Aspects of Cyber-Attacks in the Context of the Pandemic Covid-19

The home isolation of millions of employees around the world, who have been forced to work from home as a measure to limit the spread of the COVID-19 virus, has led to an increase in cyber-attacks and attempted digital intrusions.

[1] Ministry of Finance, Romania, Address: 16 Libertății Blvd, District 5, Bucharest, Romania, Corresponding author: vladimir.virgolici@gmail.com.

[2] Ministry of Finance, Romania, Address: 16 Libertății Blvd, District 5, Bucharest, Romania, E-mail: alina.ionita@mfinante.gov.ro.

[3] Regional Transport Police Department, Romania, Address: 1 Strada Gării, Galati 800222, Romania, E-mail: draganescu_alexandru@yahoo.com.

[4] General Directorate of Gendarmes of the Municipality of Bucharest, Address: Strada Jandarmeriei 9-11, Bucharest, Romania, E-mail: catalin.stegaroiu@mai.gov.ro.

The spread of the coronavirus on all continents and the emergence of the pandemic have created the perfect environment for hackers. Thus, the employees who were isolated at home used home internet networks that were less secure, and sought to inform themselves about the coronavirus.

This created a security loophole that malicious individuals could abuse. They resorted to email phishing or psychosocial manipulation online to gain access to or steal sensitive information from millions of people, who they tried to adapt to working remotely and didn't have their equipment properly secured and configured. For people who have worked and still work in a “telework” regime. I believe that the threat regarding IT security is similar to that which exists in cafes, restaurants or airports, because at home we do not benefit from the security that we find at our workplace.

Hackers are capitalizing on the fear of COVID-19 and causing many users to access malicious attachments or links. They take advantage of the emotional element by creating fake crowdfunding sites for people affected by the coronavirus.

At the same time, we must take into account that Phishing is the most well-known form of fraud on the Internet. Through such fraud, they create fake copies of well-known websites such as an email service, a social network, an online banking website, etc., through which they try to attract users.

The latter register on these websites, entering registration data and passwords that later end up in the hands of cybercriminals. Many personal, bank account data or captured passwords are used to extort money from users or send specific spam message and malware files through compromised email accounts or through social networks.

Phishing is probably unique among computer scams.

In order for a phishing scam to be successful, the tacit consent of the victim to participate, even involuntarily, in this action is necessary. This acceptance consists of the victim's response to the phisher's request to provide personal information, via an email, website, or phone call. If the victim doesn't cooperate, the scam doesn't happen.

As general methods of combating, we consider the following to be useful: no security, confidential, personal information will be provided in response to any email. If the requests come from an e-mail that appears to be from a financial institution with which you have an account, it is preferable to call the institution directly using the number on its website; o awareness of family members not to respond to such e-mails, a single unauthorized user is enough to open the door to identity theft; o showing increased attention to testing the URL or web addresses of certain important sites, such as that of the bank, because there are many fake, “phishing” or web addresses in the online environment phaming” that wait for mistakes made by users when typing web addresses in order to capture important information related to banking data; o not passing on confidential information to those who call you on behalf of a bank or any other organization. None of them will ever ask you for such information without proving its legitimacy and the fact that it is not being used for another purpose.

2. Coronavirus Maps

Despite the disastrous spread of COVID-19, hackers have exploited every chance to prey on internet users. Thus, they took advantage and are taking advantage of the fear that gripped the whole society and spread malicious programs or launch cyber-attacks.

A report by some cyber security researchers was recently presented and highlighted that a new cyber-attack has been developed, which is based on the increased interest of internet users in information about the new strains of the coronavirus that are wreaking havoc worldwide. This malware cyberattack targeted users who searched for cartographic representations of the spread of the COVID-19 virus on the Internet and were lured into downloading and running a malicious application that in turn displayed a map of how the population was infected on globe with the pandemic virus. But this app came from a so-called safe source and subsidiarily compromised the user's device.

Following the analysis by cyber security researchers of how this malicious software is designed, it was found that the malware, which aims to collect information from users, is based on a malicious product identified as AZURult, whose software structure was created in 2016. It collects information stored in browsers, such as cookies, browsing history, user IDs with their passwords and access keys of various types of cryptocurrencies. Having at hand such data collected from users, the hackers can access bank accounts, emails, even find out sensitive information.

Analyzing the malware embedded in the file that is downloaded from the COVID-19 map website, it is named Corona-virus-Map.com.exe which is an executable type

(Win32) file with a size of about 3, 26MB. Therefore by double-clicking the file, a window opens showing information about the spread of the Coronavirus. It centers around an "infection map" belonging to a legitimate online source. The information displayed in the window is real-time information about COVID-19 from the Johns Hopkins University website[1].

Incidentally, the site is created and the data provided (the window is interactive and there are links to other sources) and thus, hackers gain the trust of the user. As for how the malware works, it runs a task scheduler so that it is difficult to identify. As for how the malware works, it runs a task scheduler so it's difficult to identify.

Once the executable is run, this results in the creation of duplicates of Corona-virus-Map.com.exe and several Corona.exe, Bin.exe, Build.exe, and Windows.Globalization.Fontgroups.exe files. Compared to the above, it modifies a number of registries and accesses multiple URLs, thus creating various network communication activities, while the malware gathers stored information from the infected environment. To better understand the above, the following image shows a sample of the malicious product's modus operandi. As for how to remove and stop the malicious program, it consists of using an up-to-date antivirus and an active firewall.

Simple user caution against files downloaded and run from the Internet are not in all cases a sure way of prevention, because in these moments of social tension created by the Coronavirus, users of Internet-connected devices are eager to know current information. Thus, they neglect all aspects of cyber security. So we can say that not only offline precaution (such as avoiding contact with the virus) is necessary, but online as well.

3. Phishing through the Visual Identity of the World Health Organization (WHO)

In a world that is hyper-connected, cybercrimes pose a considerable threat to state and citizen security. So, on behalf of the WHO, hackers and cyber crooks took advantage of the coronavirus disease (COVID-19) pandemic by sending fraudulent e-mails and messages through which they tried to make referrals to malicious links

[1] The data that is mentioned on the map is collected from the World Health Organization, the US Center for Disease Control and Prevention, the National Health Commission of the People's Republic of China and Dingxianyuan, a communication site for medical professionals.

or attachments. There have been some cases reported of people fraudulently presenting themselves as WHO or the COVID-19 Solidarity Response Fund, and/or sending invoices requesting payment on behalf of the Fund. Another thing worth noting is that the site or link uses the HTTP communication protocol and not HTTPS, which is unusual for an organization of the caliber of the World Health Organization.

The COVID-19 pandemic has highlighted the need for better security in the digital world. People have increased their online presence to maintain personal and professional relationships. Speculating on this opportunity, hackers took advantage and launched attacks targeting e-commerce, electronic payment financial institutions, as well as the private and public healthcare system.

Our daily lives are connected to a wide range of services – for example financial services, transport, energy, but also healthcare (including here the world health organization).

The latter type of services is based on the physical infrastructure and, equally, on the IT infrastructure, which determines the amplification of the risks regarding a potential disruption. Since the outbreak of the COVID-19 pandemic, new technologies have made it possible for several public services of some companies to be carried out remotely via the Internet. But this realization has opened the door to an exponential increase in cyber-attacks in an attempt to maximize criminal intent by taking advantage of the disruptions caused by the pandemic and changes to traditional, physical office work. The shortage of goods was the catalyst in the development of organized crime. The consequences could have been catastrophic, in the context in which the essential services involving public health would have been disrupted, through an enormous pressure given by the pandemic.

The fear instilled by the Coronavirus proved extremely profitable for criminals in the IT space during this period, in the context of which health institutions were struggling to test patients, treat those infected and protect their staff from contamination.

As a result, phishing campaigns have appeared worldwide that try to collect money from users who want to learn about this issue.

4. Recommendations

Given that cyber-attacks and computer crime are constantly increasing, especially in times of crisis such as the Covid-19 pandemic, I propose the following recommendations to limit them:

1. Surfing the Internet must be done under the rule of patience and vigilance. The decision to access a link should be characterized by prudence. Successive access to links (referral links to other "information sources") in order to find out some information regarding the pandemic, must be done under the sign of circumspection;

2. Conducting own research in the online environment, on legitimate and well-known sites;

3. Verifying the veracity of the sender, since the name of the sender is not always the real one (specific to the criminal activity presented is that the e-mail is sent by the "World Health Organization"); attackers have the possibility to mask the sender and can pass whatever name they want in the sender field (from);

4. Identifying spelling and grammatical errors is a first step that guarantees the authenticity of the e-mail; from the analysis of e-mails with fake content, the idea emerges that not all attackers make typos, but a significant number of them do;

5. Checking the URL before accessing the site is another precaution; if there are doubts about the legitimacy of the site it is recommended not to enter personal data or download resources from it. In the online environment there are tools for checking some sites or files, such as Cockoo, VirusTotal, Sandbox, etc.;

6. Not transmitting such data on sites that are built with the purpose of raising awareness about public health issues because they do not ask for personal data, e-mail address, let alone passwords;

7. Changing your password if your password has been transmitted to a compromised site, as cybercriminals will use it to access other accounts;

8. Using multiple passwords when logging in to various accounts in the online environment;

9. Using of multi-layered security measures where devices enable, for example, two-factor authentication through applications that generate six-digit numeric codes that are transmitted to the phone.

References

Acronis (2021). *Acronis Cyber threats Report 2022 unveils cyber-threat predictions*. https://www.acronis.com/en-us/blog/posts/acronis-cyberthreats-report-2022-unveils-cyberthreat-predictions/.

CISA (2021). *AA21-265A-Conti Ransomware TLP White*. https://www.scribd.com/document/529330620/AA21-265A-Conti-Ransomware-TLP-WHITE.

ENISA (2021). *Enisa Threat Landscape 2021*. https://www.enisa.europa.eu/publications/enisa-threatlandscape-2021.

UNODC (2021). *Digest of Cyber Organized Crime*. https://www.unodc.org/documents/organizedcrime/tools_and_publications/21-05344_eBook.pdf.

Surdu, Ileana-Cinziana (2018). Cybersecurity. Risks, Threats, and Trends of Manifestation in Romania. *International Conference RCIC'18*, pp. 365-372. https://www.afahc.ro/ro/rcic/2018/rcic'18/volum_2018/365-372%20Surdu.pdf.

Hive Ransomware Attackers Extorted $100 Million from over 1,300 Companies Worldwide. https://thehackernews.com/2022/11/hive-ransomware-attackers-extorted-100.html.

COVID-19, Info Stealer & the Map of Threats; Threat Analysis Report, https://reasonlabs.com/blog/covid-19-info-stealer-the-map-of-threats-threat-analysis-report.