INFINITY

IMMERSE. INTERACT. INVESTIGATE.

Policy Brief

Current cybercrime situation in Belgium

DISSEMINATION LEVEL PUBLIC

PARTNER

Antwerp Police

AUTHOR

Aileen Moorkens

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No. 883293. The content of this document represents the view of the authors only and is their sole responsibility. The European Commission does not accept any responsibilty for any use that may be made of the information it contains.

Policy Brief

Current cybercrime situation in Belgium

1. Cybercrime Situation in Belgium

The Belgian National Risk Assessment 2018-2023 of the National Crisis Centre considers cyber as one of the main risk clusters our country will be facing in the upcoming years. Within this cluster, cybercrime and hacktivism that targets enterprises and critical infrastructures are identified as national priority risks. Moreover, the evolution of the cyber threat from financially driven to geopolitically motivated is extremely concerning. Western countries are facing a threat in cyberspace that exceeds the danger of physical attacks. These cyber threats can have severe direct effects on, for example, our electricity distribution, our banking systems, or on the availability of all online services. Continued coverage of cyber incidents, even minor ones, can cause the public to lose confidence in the digital environment and services, which could result in pernicious economic consequences.

The cyber threat, as part of the hybrid threat, can be used to amplify the effects of other methods of attack. In the case of this threat, a combination of, for example, a physical attack with a series of cyber-attacks can seriously amplify the impacts and temporarily create an atmosphere of chaos. Cybercrime represents 1 of the 4 main elements of the threat landscape in Belgium. Belgium considers the following actors to pose the greatest threat to the Belgian state and its population: cybercriminals, foreign military and intelligence services, terrorist groups and hacktivists. These are not just threats that could disable our infrastructure, but they can affect the integrity, accessibility, and confidentiality of the information that we digitally capture, analyse, and exchange as well.[1]

2. Cross-cutting cybercrime facilitators

2.1 Financing through crypto

The current developments also indicate an increasing use of cyber tools for financing terrorism, e.g. through cryptomining or even crowdfunding. Over the past few years, many new cryptocurrencies have emerged with corresponding logos or symbols that can be recognized online, on social media, through apps on smartphones or in propaganda.[2]

Simultaneously, we are witnessing an increase in the use of cryptocurrencies for criminal purposes. Pseudo-anonymity and decentralization provide an appealing setting for criminals. Not only do virtual currencies enable rapid international transactions, they also provide the opportunity to exploit regulation loopholes between jurisdictions.[3]

Figure 1: Cryptocurrency examples: https://bit.ly/3JVBwm1

The criminal use of cryptocurrencies is no longer limited to the phenomenon of money laundering and cybercrime. It now extends to all forms of crime of which the transfer of money is a part. Thus also in the financing of terrorism. The costs for transactions abroad are considerably lower, which makes virtual currencies interesting for sponsoring extremist and terrorist groups abroad. The use of cryptocurrency for terrorist financing is of particular interest to organizations whose access to the regular banking system is limited. Although the use within terrorist groups so far remains rather limited and unsystematic.[4]

3. Phishing and social engineering

The public health crisis of 2020, better known as the COVID-19 pandemic, marked the starting point of a significant increase in the popularity - or notoriety - of phishing attacks. As a phenomenon, the pandemic continued to affect every part of our daily lives throughout 2021.

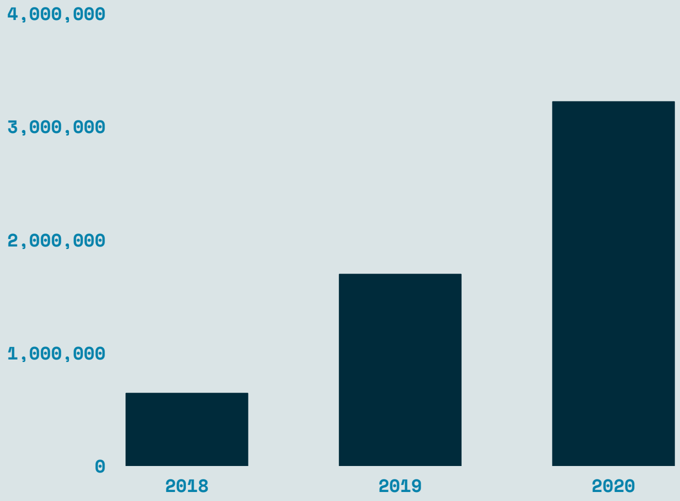

Figure 2: Number of reported phishing messages at verdacht@safeonweb.be

Meanwhile, hackers and other malicious actors efficiently adapted their modus operandi to even better suit our new and formerly unusual way of living and working. The corona pandemic has opened the door permanently to a continuous increase in phishing threats. The pandemic pushed businesses and individuals to adjust to this new reality.[5] In 2021, as much as 23% of all Belgian employees were victims of phishing scams.[6]

These adjustments were prompted by, among other things:

- Increased anxiety, uncertainty and emotions due to COVID-19
- Inexperience with working from home, from both employee and employer perspectives
- Including the need to quickly implement new software tools and protocols and train users

Phishing is at the base of the vast majority of all cyber breaches in Belgium. 'People don't think, they click', especially when:

- The phishing message is short and to the point
- The message contains a request for help
- The sender appears to be known to the recipient (the likelihood of a click increases by 30%)
- The phishing message contains a reference to a hot topic

Most phishing messages concerned the following topics[7]:

- COVID-19 (work at home, testing, vaccination)
- HR-related (fines, termination, leave, sensitive content)
- Supplies (Deliveries, Amazon, bol.com, Coolblue)
- IT-related (passwords, VPN, IT support)
- Office-related (Microsoft, Gmail, SharePoint)
- Management (e.g. spear phishing , CEO fraud)
- Finance-related (e.g. invoices)
- News

4. COVID-19 catalysator

The COVID-19 pandemic renders individuals and society extremely vulnerable in all respects. During this crisis, we all relied more than ever on computer systems, mobile devices and the internet to work, communicate, shop, share and receive information and otherwise mitigate the impact of social distancing. In terms of cybersecurity, the COVID-19 pandemic also had an impact. By means of e-mails on COVID-related topics people are persuaded to provide certain data. Capitalizing on topical issues is a well-known tactic of cybercriminals, especially if the issue in question is coupled with uncertainty and fear.[8] Similarly, given the need for certain certificates in multiple sectors, a business of various counterfeit certificates has emerged. For example, QR codes and recovery and vaccination certificates are sold through social media.[9]

The most recent COVID-19 related cybercrime events were false reporting, ransomware through Tracker App, phishing messages surrounding COVID-19 testing and tracing.[10] [11]

4.1 False reporting concerning COVID-19

Cybercriminals spread viruses and ransomware hidden behind COVID-19 messages and applications. These messages are sent via WhatsApp, Facebook, Instagram and all other social media. Most of the messages are about following topics:

- Offers for face masks, alcohol gels, disinfectants etc.
- Links to fake news sites
- Fake fundraising campaigns for victims of the virus
- Messages that appear to come from health organizations and contain a link to a fraudulent website that then requests your information
- Emails originating from your bank
- Messages relating to corona crisis compensation

4.2 Ransomware COVID-19 Tracker App

The COVID19 Tracker App allows you to apparently track cases of COVID-19. In reality, the app was infected with ransomware, named 'CovidLock'. CovidLock uses techniques to deny the victim access to his or her phone. A password change occurs to unlock the phone which makes your own password ineffective. After this, you are immediately presented with a screen explaining how you must pay $100 in Bitcoin within the 48 hours. If you don't, all data will be deleted from your device and they threaten to publicly leak all your contacts, photos, videos and all social media accounts onto the internet.

4.3 Phishing messages

The past two year there has been an increase in victims of phishing tactics. The number of COVID-19 related phishing attempts conducted above all via telephone (vishing) and text messages (smishing) have risen considerably. Consequently, the past two years have witnessed a huge increase in victims of these phishing tactics. Especially concerning false reports that are circulating around COVID-19 testing and tracing.

5. Cyber-dependent crime

5.1 Malware[12]

Malware remains a key element within cybercrime. Between August 2019 and January 2020, Belgian companies suffered between 200 and 550 attacks per month. The web is the largest source of malware, responsible for 53% of attacks, mail accounts for 47%. The files used by attackers to target our country are also different in nature. Looking at mail-based infections, Word files are the most popular vector. When spreading malware via the web, files with a cmd extension comprise the largest share. Such batch files can contain powerful commands which, especially with the correct rights, can cause a great deal of damage to a system and can autonomously introduce new malware.

Emotet remains the most popular type of malware. Emotet is a trojan horse that originated as banking malware, but has since been used as a vector to spread all kinds of malware. The malicious software spreads mainly via phishing links and accounted for 11% of the detected attacks in Belgium.

5.2 Ransomware

Ransomware is a very aggressive type of attack carried out by cybercriminals. The impact of a ransomware attack can be devastating, companies spend millions to restore business continuity. Some organizations give in to the demand for ransomware because restoring business continuity is time-consuming and therefore costly. The targets of ransomware attacks are becoming increasingly large-scale such as hospitals, critical infrastructures, government agencies, etc. Recently, there were a few ransomware attacks on hospital networks.[13]

Over the past year, we have noticed a significant increase in the number of ransomware cases. Although they already date back to 2017 and 2018, WannaCry and NotPetya are still fresh in our memories. It was the first time that the effects of a global ransomware attack was felt in Belgium. In 2020 we were startled by a new family of ransomware called Anatova.[14]

6. Child sexual exploitation online

Following the different lockdowns young people were much more active online and therefore more exposed to online risks. The number of cases of minors whose sexual integrity was compromised increased during this period by a factor of 3: grooming, sextortion or cross-border sexting. We also witnessed a tripling in the amount of reports made through our civilian hotline (stopchildporno.be) during the first lockdown. Underlying was an increased demand, an increased exchange, but also an increased production of such material.[15]

There has been a steep increase in online grooming activities on social media and online gaming platforms. The production of self-generated material is a key threat since this material is displaying increasingly younger children. Overall activity related to child sexual abuse material (CSAM) distribution on P2P networks has increased considerably.[16]

7. Criminal abuse of the dark web

The Darknet is the Wild West of the Internet. The dark place where criminals anonymously set up their dubious businesses, CSAM are exchanged and terrorists prepare an attack without interference. But it is also an illegal shopping center where you can buy everything that is forbidden above ground: from hard drugs to a Kalashnikov. The supply of substances, sold from Belgium, lies in line with global trends. XTC pills and MDMA (the active ingredient in xtc) are the most frequently and stably offered in these markets, followed closely by other stimulants (cocaine, speed) and cannabis.[17] Illicit drugs remained the main commodity traded on the dark web.

Its users are increasingly using Wickr and Telegram as providing a platform for discussions, sharing information on vendors en costumers or to bypass market fees.

8. Some general CC statistics

The Center for Cybersecurity in Belgium (CCB) supervises, coordinates and monitors the implementation of Belgium's cybersecurity strategy. Within the CCB, the Computer Emergency Response Team (CERT.be) is responsible for detecting, observing and analyzing online security problems.

To manage cybersecurity incidents and crises on a national level, there is the National Cyber Emergency Plan. For this, the National Crisis Center works together with the Center for Cybersecurity Belgium and other government partners. This allows all these partners to work together in a coordinated way to protect our country's important sectors from cyber-attacks.[18]

8.1 LEA capacity

Criminality follows the evolution of society and takes advantage of technical and technological developments. Cybercrime is therefore a phenomenon that is only growing and from there the importance of specialized units in this domain is only increasing. While ICT criminality and related investigations were the domain of specialized investigators in 2001, they are now part of the daily operation of every police officer.[19] To counter the rising threat of cybercrime in Belgium it is necessary to increase the capacity of specialised cybercrime units at both the federal as the local police levels.

8.2 International cooperation

On Belgian territory, there are frequent events with an increased cyber risk such as an international summit, elections, major European and international events and organizations. The cyber threat is global and cannot be dealt with solely at the national level. International cooperation is a key component of a decisive national cybersecurity policy. Particular attention is paid to the agency for cybersecurity in Europe, ENISA. Since its establishment in 2004, ENISA has been developing an overall culture and awareness for network and information security in Union. The CCB will continue to represent Belgium in the various bodies and platforms of ENISA.[20]

Furthermore there is also the Cyber Security Coalition which is a unique partnership where stakeholders from the academic community, public agencies and the private sector work together in the fight against cybercrime. By 2021, more than 100 key organizations from across three sectors are active members, contributing to the mission and goals of the coalition.[21]

In recent years, there has been an increase in law enforcement coordination via international initiatives. For example, Belgium is a member of the Joint Cybercrime Action Taskforce (J-CAT) which has completed 25 operational actions in 2021.[22]

References

1. CCB. (2021). Cybersecurity strategie België 2.0 2021-2025. Retrieved on March 23, 2022, from https://bit.ly/3tPIfsy
2. First Responders Toolbox (2021, 23 September). Identifying and Preventing Illicit Use of Cryptocurrency by Terrorists. Retrieved on March 22nd 2022, from https://bit.ly/35T8DIw
3. Europol (2021). Cryptocurrencies - Tracing the evolution of criminal finances. Retrieved on March 8 2022.
4. Europol (2021). European Union Terrorism Situation and Trend report. Retrieved on March 2 2022.
5. PHISHED (2021). 2021 Phishing Intelligence Report. Retrieved on March 23 2022, from https://bit.ly/3JItPQt
6. Vlaanderen. (2021). Dit was phishing in 2021. Retrieved on March 25 2022, from https://bit.ly/3qLepmR
7. Ibid.
8. VANROEY (2021). Opgelet: cybercriminelen misbruiken COVID-19 voor phishing. Retrieved on March 3 2022, from https://bit.ly/35vdcZn
9. VRTNWS (2021, 23 november). De sluipwegen naar een coronapas: van besmettingsafspraakjes tot handel in valse certificaten. Retrieved on March 20 2022, from https://bit.ly/3rLIGBC
10. Ibid.
11. Politie.be. (2021). Cybercriminaliteit met betrekking tot het coronavirus COVID-19. Retrieved on March 15 2022, from https://bit.ly/3wIf6kM
12. Aussems, M. (2020). Malware in België: klikken op exe's en cmd's populair. Retrieved on March 25 2022, from https://bit.ly/3IOmIVj
13. CERT. (2020). Ransomware, een use-casegebaseerde aanpak. Retrieven on March 25 2022, from https://bit.ly/3tP53IX
14. CERT (2020). Laat België niet lamleggen door ransomware. Retrieved on March 22 2022, from https://bit.ly/38aEfKK
15. Child Focus. 2020. Jaarverslag 2020. Retrieved on 25 March 2022, from https://bit.ly/3IMy5gr
16. Europol 2021. Internet Organised Crime Threat Assessment. Retrieved on 22 March 2022, from https://bit.ly/36CTxrd
17. Colman, C. (2018). De grens voorbij-Belgische en Nederlandse drugsmarkten in beweging. Retrieved on March 29 2022, from https://bit.ly/3I0103I
18. CCB. (2021)
19. Politie.be. (2021) Federal Computer Crime Unit. Retrieved on March 15 2022, from https://bit.ly/35ntN1q
20. CCB. (2021)
21. Ibid.
22. Europol 2021. Internet Organised Crime Threat Assessment. Retrieved on 22 March 2022, from https://bit.ly/36CTxrd