INFINITY

IMMERSE. INTERACT. INVESTIGATE.

Policy Brief

The cybercrime situation in Portugal

DISSEMINATION LEVEL PUBLIC

PARTNER

PJ

AUTHOR

Lúcia Lebre

António Fonseca

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.

1. Cybercrime Situation in Portugal[1]

1.1 General Background

The frequency and reach of threats and cyber-attacks is increasing in Portugal and across the world. The COVID-19 pandemic favoured some intrusive actions, taking advantage of technical vulnerabilities and the circumstances of remote working as increasing conversions from offline crime to online crime. The greater number of communication terminals and portable computer systems, and the longer connection to cyberspace (always on), associated with confinement, contributed to greater exposure to technology-based attacks, namely in the serious and serious forms called 'RAT' (remote access trojan), 'APT' (advanced persistent threat), encryption (ransomware) and data deletion combined with computer sabotage.[2]

In line with previous years, it appears that Phishing and Smishing attacks remain dominant. There was a rise in the number of Phishing, Smishing and Vishing (43%) campaigns as well as threats of ransomware, fraud and online scams in which social engineering and exploitation of the human factor are key elements. Various forms of fraud and deceit as fake phone calls on behalf of Microsoft, sextortion (26%), as well digital disinformation, were threats that also materialized through the manipulation of perceptions, taking advantage of people's greater isolation and the growing need for digital caused by the pandemic.[3]

The second highest classification of incidents was Malicious Code, although with a slight decrease compared to the previous year. In this class, Infected Systems (infected PC, smartphone or server) and Malware Distribution (URI used to distribute malicious code) stand out, both associated with different families of malicious codes (FormBook, Agent Tesla, Lokibot, among others).[4]

With regards to the significant increase in incidents in the Information Collection class, where Social Engineering attacks are predominant, the most common cases are Sextortion, Vishing and CEO Fraud.[5]

Current cybercrime situation in Portugal

April 2020 and February 2021 were the months with the most recorded cybercrime reports. These months correspond to periods of greater social confinement as a result of the COVID-19 pandemic.[6]

The most common sources of cybercrime are human error (43%), ransomware (22%) and deceitful actions (13%). The main victims of cybercrime have been the commerce and services sector, banking (13%), infrastructures (8%), Service Providers (6%) as well as citizens in general.

The percentage of computer-related crimes registered by police authorities grew by 6% in 2021 compared to the previous year, although the number of strictly computer-related crimes decreased by 11%.[7]

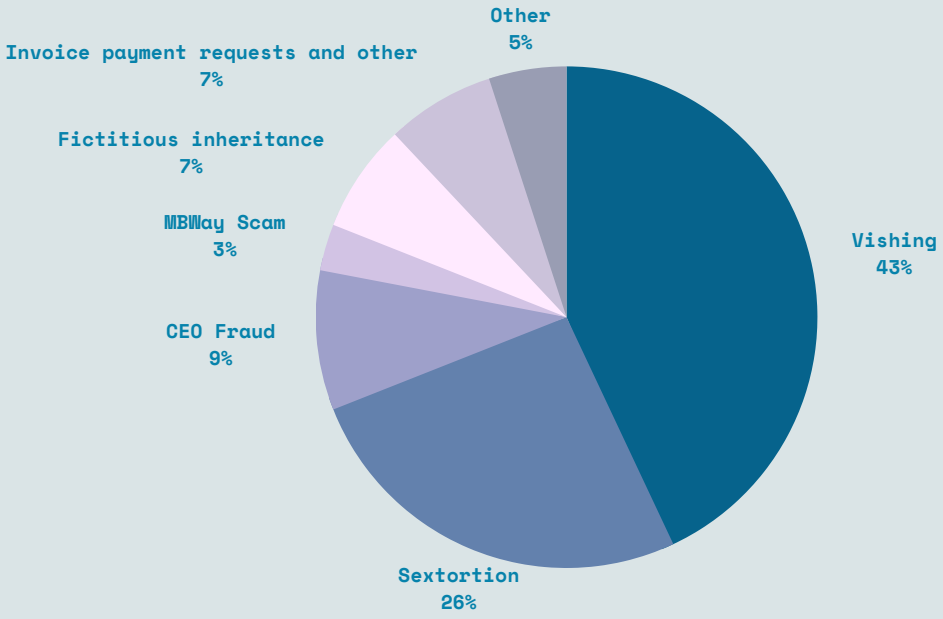

Figure 1: Social engineering cases in Portugal in 2021[8]

Although the amount of computer-related crimes had grown in 2021 by 6%, a Eurobarometer study on cybercrime, on the Awareness and Experience of Cybercrime, published in 2020, noted that only some 41% of Portuguese respondents are saying they feel very "well informed" against 57% "not well informed" and are consistently amongst the least likely to report being a victim of cybercrime.[9]

These rather low figures figures correspond to the European Cybersecurity Index of 2021, an in-depth study by the UK-based cybersecurity company ESET, revealing the countries in Europe with the best and worst levels of online safety. Seven factors of cybersecurity that had been analysed for 24 European countries, included the number of pieces of cybersecurity legislation, the percentage of each country's residents who've fallen victim to bank card or online banking fraud in the last three years, and the percentage in each nation whose social network or email accounts were hacked in the last three years. According to this study, Portugal boasted very low numbers of people who have fallen victim to malicious software, social media hacking, online banking fraud and identity theft. This, coupled with legislation in five categories (national strategy, content, privacy, critical infrastructure and commerce), earned Portugal its title as the best European country for cybersecurity.[10]

2. Cyber-dependant crime

With regard to cyber-dependent and cyber-instrumental crime, the main modi operandi are associated with the crime of money laundering resulting from false investment fraud, CEO/Mandate Fraud scams, online fraud (associated with the transaction of goods or services), Phishing, in particular Banking Phishing, and whose commitment is increasingly organized.

Banking Phishing, using the modality of Smishing (sending an SMS with a link) and Vishing (phone call to validate data or illicitly made bank transfer), and online scams, whether in investments in virtual currency or through the transaction of goods or services, continue to predominate.

In this type of malicious action, the use of the image of institutions in the banking sector, financial services, transport and logistics institutions is prominent, entities providing electronic mail services and also state services. The dissemination of these campaigns is mostly carried out via email messages (Phishing) and, to a lesser extent, but growing, via text or multimedia messages via mobile devices or applications (Smishing). The purpose of these campaigns is, mainly, the collection of access credentials to homebanking and financial services, the collection of credit or debit card data and the collection of access credentials to electronic mail (for exfiltration of information and/or dissemination fraud campaigns, originating from a trusted e-mail).

Exploitation of criminality associated with blockchain-based technologies, illegitimate access to cryptocurrency wallets, increased obfuscation of criminal intentions through forms of malicious programs linked to extortion (ransomware) with the true aim of sabotage is foreseen.[11]

3. Cyber espionage

In 2021, there was continuity of several outbreaks of offensive cyber operations against national targets, originating from a wide range of threat agents to develop cyber espionage operations and campaigns, in various domains. The objectives pursued consisted of accessing sensitive information, sabotaging, destabilizing and affecting the credibility of entities and individuals globally, but particularly in countries in the Euro-Atlantic area.

Indeed, the fact that more organizations are depending on digital services to ensure remote work has increased the risk of operational failures, which was taken advantage of by those agents.

Among the various threats to cyberspace of national interest, four foci of insecurity must be highlighted: cyberespionage, disinformation, cybercrime and hacktivism.[12] These attacks [13] have been attributed, in part, to cyber groups located in other countries, with the aim of accessing the computer systems of public and private entities to exfiltrate privileged information (personal data),[14] intellectual, industrial and commercial property). In this context, ransomware attacks took on particular relevance, which had a substantial growth, having been observed, in many circumstances, that the attackers managed to access and temporarily disrupt the functioning of critical infrastructures in the energy sector. Along the same lines, an increase in incidents of compromise of supply chains of technological products/services to access customer data was also identified.[15]

In the universe of cyber espionage against Portuguese targets, there was continuity in the occurrence of cyberattacks aimed at compromising public and private targets, as well as entities with strategic relevance, in order to exfiltrate classified, sensitive or privileged information. It was a persistent threat with the possibility of development, with regard to the sophistication, volume and disruptive consequences of these actions. In the field of cybercrime, a trajectory of increased threat was noted, namely when motivated by the growing professionalization of highly organized transnational cybercrime committed to extortionist activities or digital fraud that included Portuguese cyberspace among its attack surface. It should also be mentioned the actual worsening of international cybercrime operations against the Portuguese digital fabric, with consequences of increasing public visibility and with a potential to disrupt social and/or economic dynamics, namely in the context of ransomware operations.[16]

It is important to consider the threat from external and domestic hacktivist circles. This is a wide and diffuse universe of threat agents that, despite their technical limitations, ensured, in the course of 2021, the execution of destructive and media attacks against institutional targets, for the purpose of promoting reputation among their communities of reference and Portuguese society.

4. Payment fraud

The phenomenon of fraud through electronic means of payment has registered a continuous increase, as a result of the proliferation of the use of digital technologies, electronic commerce and easy-to-use applications (allowing simple and fast payments), but not always accompanied by secure procedures as the case of double validation, or with “security flaws” /absence of secure validation procedures by banking entities, payment processors and merchants, which easily allow anyone to use someone else’s payment data.

This new reality produces and concentrates a high number of inquiries for investigation. On the other hand, given the emergence of criminal phenomena such as the case of fraud through the MB Way application, the situation has become more serious. Despite the impact of the crime (low value and little criminal and penal relevance), the phenomenon reached thousands of victims who were left in serious financial difficulties.

In the specific case of fraud using electronic means of payment, implementation/consummation tends not to be highly complex, and any citizen with average knowledge of the digital environment may be the author of fraud, even when dealing with cases of skimming (aka cloning of cards) or logical attacks, because the complex process is not the realization, but the construction of devices and/or computer programs/malware, actions (these yes) planned and executed by experts.[17]

With regard to actors, there is a sharp decrease in groups originating in Eastern Europe and engaged in 'Gift Card' fraud by making, in a short period of time, a large volume of low-value payments. It is admitted that police action in this domain has led these groups to move their activity to other countries. On the other hand, a large increase in the number of Brazilian networks operating in Portugal is beginning to be noticed, which can be seen from the fact that most of the detainees in the last 18 months are of that nationality.[18]

2021 was also marked by relevant developments in the field of cryptocurrencies, whose interaction with economic activity has been intensifying, reinforcing the debate on the urgency of adopting digital currencies and, above all, their regulation by States.[19]

5. Child sexual exploitation online

With regard to the criminal phenomena of abuse and sexual exploitation of minors online, it appears that Portugal is confronted with some of the fundamental vectors identified in the Europol Internet Organized Crime Threat Assessment (IOCTA) report, namely:

- >> The self-production of intimate content as a result of enticement phenomena and/or coercion phenomena;
- >> The production, sharing and hosting of illegal content on encrypted platforms; sharing illegal content on peer to peer (p2p) networks;
- >> The sharing, in some cases viral, of illegal content on social platforms;
- >> The use of platforms that especially enhance anonymity on the darknet, and the abuse and sexual exploitation of minors by viewing them from a distance with a commercial nature.

Online abuse situations, at least in the Portuguese case, tend to be committed by isolated individuals, generally Portuguese or resident in Portugal, so they do not assume the characteristics of international organized crime, even though, due to the nature of the vehicles used for perpetration, they signal the feeling belonging to an unorganized group.

With regard to the profile of perpetrators, these crimes continue to be committed in the privacy of perpetrators who relate to each other almost exclusively online. It should be noted that the contents (the images and videos themselves) result, in the overwhelming majority of cases, from family relationships or informal care between abusers and the abused.[20]

The number of images and Internet content hosted in Portugal during 2020 was 1,773 and in 2021 this had risen to 1,929.[21] With regard to the main characteristics of the modi operadi investigated, the information collected in Portugal, in this period, points to a high prevalence of distribution of pornography of minors in common communication channels, namely YouTube, Facebook, Google Drive and Instagram.[22]

There is an increase in investigations focusing on the use of online gaming platforms to entice minors to produce intimate content, maintaining the use of encrypted platforms for the exchange and storage of illegal content. Situations of production and exchange of content using the Darknet are a minority in terms of the matter investigated in Portugal. On the other hand, online abuse is a form of criminality marked by the existence of random links between dozens of countries. It should be noted that child abuse material (the images and videos themselves) is actively traded on peer-to-peer (P2P) networks and Dark Web, where cryptocurrencies are also used for payments, with law enforcement reporting an increase in for-profit distribution.[23]

6. Cybercrime investigation in Portugal

The investigation of Cybercrime in Portugal is ruled by Cybercrime Law 109/2009, of September 15, transposing to the national legal order Council Framework Decision 2005/222/JHA, of 24 February, on attacks against information systems, and adapts to national law the Convention on Cybercrime of the Council of Europe.

The Portuguese legislation in the context of computer crimes and cybercrime establishes investigation competence for Polícia Judiciária (PJ) and as International cooperation permanent point of contact ensuring the maintenance of a structure ensuring a point of contact available on a twenty-four hour, seven-day-a-week basis (Cybercrime Law). [24]

Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T) is PJ´s specialized operational unit that provides a preventive and repressive response to the cybercrime phenomenon. UNC3T is responsible for preventing, detecting and investigating crimes provided for in the Cybercrime Law.[25] Crimes practiced with recourse or by means of technologies or computer means; espionage, when committed in the form of any computer program designed to carry out harmful actions that constitute an advanced and permanent threat; cyberterrorism, in conjunction with the UNC3T unit; crimes against freedom and sexual self-determination, whenever practiced through or through a computer system; investigation through information technology; computer and communications fraud; crimes regarding interference and illegitimate manipulation of electronic and virtual means of payment.[26]

In 2021, within the framework of Europol cooperation, PJ has participated in several European projects of which stands out the IRU – Internet Referral Unit, to combat terrorist recruitment and propaganda and other associated violent extremist activities, on the Internet. The main objective is to identify flag and eventually request the removal of jihadist content.

[26]

Within Project EMMA7, PJ participated in the operation "European Money Mule Action" (EMMA) under the theme "DontBeaMule" [27] in which 8,755 "money [transport] mules" were identified and in which "precautionary measures" prevented a total loss of 17.5 million euros.

Within Project E-COMMERCE2021, operation "e-Commerce Retail Week of Action" [28] had the objective of preventing and combating crimes of computer fraud through the acquisition of goods online. Two people were arrested who had been identified "in flagrante delicto" when receiving goods acquired fraudulently.

Within Project VIDTF9 and 10 more operations,[29] the focus was on the analysis of multimedia material with content of abuse and sexual exploitation of minors with a view to identifying the victim and/or aggressor or country of production.

7. Conclusions

There is a tendency for emerging cyberthreats and threat actors to persist and it is likely that the number of incidents and online crime indicators remain high, as well as their sophistication in 2023, proliferating in a favourable context with an uncertain end. This increased perception of the risk of suffering a cybersecurity incident in cyberspace is of national interest but at the same time a perception of higher capacity of resilience.

Persistence in exploring the weaknesses of the human factor; ransomware cases; data breaches for use of login credentials; exploitation of virtual private network (VPN) vulnerabilities; and the relevance of mobile technologies and the Internet of Things as potential attack surfaces.

It is necessary to continue to invest in the security of digital processes and technologies and in raising people's awareness, with innovative strategies campaigns, so that the social spheres most exposed to the vulnerabilities of digitization can mitigate the potentially harmful effects caused by behavioural negligence in cybersecurity.

It is also important to improve the articulation between the different social actors, namely the business and the academic world, the policy makers and the law enforcers.

Regarding law enforcement, removing certain legal obstacles for investigators, namely legal barriers around the retention and sharing of data, more officers, tools and training is required.

We also believe that the articulation with the media is relevant for the dissemination of good prevention practices in some types of cybercrime.

References

1. This Policy Brief was prepared by the Innovation and Development Division (DSID) of the Polícia Judiciária of Portugal, as part of T10.5.
2. Cf. Sistema de Segurança Interna (SSI), 2021, Relatório Anual de Segurança Interna 2021 (RASI), p.62, at: https://www.portugal.gov.pt/downloadficheiros/ficheiro.aspxv=%3d%3dBQAAAB%2bLCAAAAAAABAAzNLI0NgcAIUgtZwUAAAA%3d.
3. Cf. Centro Nacional de Cibersegurança (CNCS), 2022, Relatório Cibersegurança em Portugal, p. 4, at: https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2022-obciber-cncs.pdf.
4. Cf. SSI, 2021, RASI, p. 90.
5. Cf. SSI, 2021, RASI, p. 90.
6. Cf. CNCS, 2022, Relatório Cibersegurança em Portugal, p. 50.
7. Cf. CNCS, 2022, Relatório Cibersegurança em Portugal, p. 11.
8. Figure 1 based on data provided in: CNCS, 2022, Relatório Cibersegurança em Portugal, p. 8.
9. Cf. European Commission, 2020, Eurobarometer, at: https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableId=71905, pp.16 and 24.
10. Cf. ESET, 2021, European Cybersecurity Index: European Countries with the Best and Worst Cybersecurity, at: https://www.eset.com/uk/about/newsroom/blog/european-cybersecurity-index-2021/.
11. Cf. SSI, 2021, RASI, p. 63.
12. Cf. SSI, 2021, RASI, p. 32.
13. Cf. Diário de Noticias, 2022, at: https://www.dn.pt/sociedade/ciberataque-a-tap-dados-pessoais-de-costa-ventura-paulo-portas-e-diretor-do-sis-divulgados-na-dark-web-15190439.html.
14. Cf. SSI, 2021, RASI, p. 30.
15. Cf. SSI, 2021, RASI, p. 33.
16. Cf. SSI, 2021, RASI, p. 64.
17. Cf. SSI, 2021, RASI, p. 64.
18. Cf. SSI, 2021, RASI, p. 32.
19. Cf. SSI, 2021, RASI, p. 64.
20. Cf. CNCS, 2022, Relatório Cibersegurança em Portugal, p. 53.
21. Cf. SSI, 2021, RASI, p. 63.
22. Cf. SSI, 2021, RASI, p. 63.
23. Cf. Polícia Judiciária, Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T), at: https://www.policiajudiciaria.pt/unc3t/.
24. Cf. Lei do Cibercrime https://dre.pt/dre/detalhe/lei/109-2009-489693.
25. Cf. Polícia Judiciária, Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T).
26. Cf. Europol, 2021, European Money Mule Action (EMMA), https://www.europol.europa.eu/media-press/newsroom/news/european-money-mule-action-leads-to-1-803-arrests.
27. Cf. European Association for Secure Transactions (Global) Ltd., 2022, Thousands of Money Mules arrested in international Police Operation, at: https://www.association-secure-transactions.eu/thousands-of-money-mules-arrested-in-international-police-operation/.
28. Cf. Polícia Judiciária,Operação "e-Commerce Retail Week of Actio, at: https://www.policiajudiciaria.pt/operacao-e-commerce-retail-week-of-action/.
29. Cf. SSI, 2021, RASI, p.131, in: https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBQAAAB%2bLCAAAAAAABAAzNLI0NgcAIUgtZwUAAAA%3d.