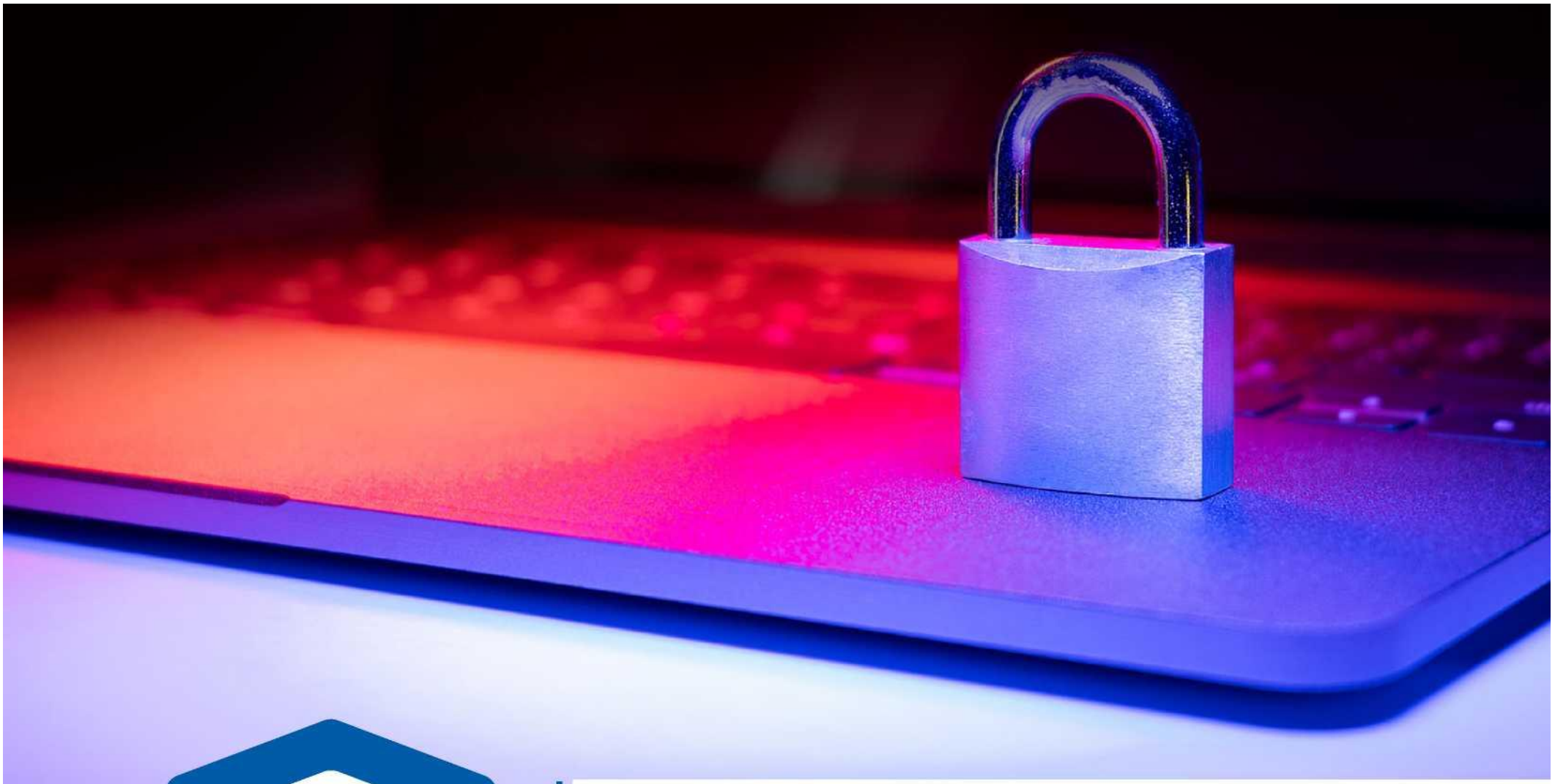

PTSOC 2023 Annual Report "Year of Ransomware"

Índice

Framing

In 2023, in a global context where cybersecurity incidents and cybercrime continue to increase in number and sophistication, with ransomware, online scams and social engineering techniques such as phishing, smshing andmore recently quishing, with the use of QRCodes, leading the cyber threat framework. These techniques amplified by the advances in Artificial Intelligence (AI) and machine-learning (ML), will allow you to analyse and process large volumes of data, in real time, automating and introducing greater sophistication into these typologies of attacks.

This trend is reinforced in the World Economic Forum's 2023 Global Risk Report, which anticipates the spread of cybercrime and cyber insecurity as two of the top 10 global risks in the coming years and raises cyber(in)security as one of the key issues to be addressed by the European Community on the European Union's (EU) 2030 Digital Decade agenda.

This annual PTSOC report aims to present a brief overview of the main events and trends observed in 2023 in the areas of cyber security and to put into perspective the main challenges ahead of 2024.

CHAPTER 2

2.

Major cyberattacks of 2023

January

Royal Mail, a British postal company, was the subject of a **ransomware** cyberattack, which led to the interruption of **international parcels and letters** for more than a week with a significant impact on its operations.

The **Super Bock** group has

February

been the target of a **ransomware** cyberattack which has led toconstraints on the **supply** of some of its products on the commercial market.

The website of the **French National Assembly** was attacked by **DDoS** by a group

March

of pro-Russian hackers **causing its temporary unavailability**.

April

Samsung employees unintentionally **exposed internal code and internal meeting notes by using OpenAI's 'ChatGPT'** tool to help them identify errors andproduce meetings.

The **Polytechnic Institute of Leiria** suffered a computer attack that caused 14 thousand students to run out of internet access in schools and residential homes. That attack ultimately led to instability in its services,namely the **unavailability of all the institution's online activity**.

Globalcaja**,** based in the Spanish city of Albacete, was the subject of a computer attack (Ransomware) which **blocked several offices and took place the exfiltration oftrust data, customer and employee documents, passports and contracts**. The Play ransomware group re-invited the attack.

NATO suffered a phishing campaign focusing on the Nato Summit that took place in Vilnius, Lithuania, on July 11-12. This hack used **typosquatting techniques and spear-phishing emails** with theobject of infecting participants with malware.

Several Italian banks were attacked by DDoS. The national cybersecurity agency in Italy has confirmed that at least five Italian-banks have been targeted by cyberattacks. Those attacks **caused unavailability on the websites ofthose banking entities and were inaccessible**. The pro-Russian group Noname was identified by theItalian authorities as having been the malicious actors responsible for these attacks.

may June July August

The municipality of Gondomar, on September 27, was the target of a cyber attack, forcing the authorities to put the systems offline and contact the National Cyber Center and the National Data Protection Commission. Rhysida ransomware gang, the author of the cyberattack,leaked passports and-financial documen after the ransom was not paid.

DNA testing company 23andMe reported **in** October that access to biometric dataof 5.5 million customers was not allowed. The malicious actors used previously promised accountsto carry out a "***credential stuffing***" attack. This type of attack could have been avoidedby customers through the non-reuse of passwords. This incident also led to the need for companies to proactively analyse the security of their users' accounts.

North American aerospace-development and defense multinational **Boeing** suffered a cybersecurity incident by the LockBit ransomware gang where about 43 GB of data were published online. The incident presented no threats to aircraft or aviation security.

On December 10, EasyPark**,** a car parking company, reported that it was the target of an informantattack where malicious actors had access to their customers' personal information such as name, mobile phone number, address, email address and partial debit/credit card number. Despite the incident, the company acted quickly and correctly, changing the password and notifying its customers and competent authorities in a timely manner.

Septemb er

October

November

December

3

Main cyber threats in 2023

CHAPTER 4

Ransomware

The year 2023 was marked by the growth in the supply of Ransom-ware-as-a-Service (RaaS) services. This business model has become particularly lucrative and cyber-criminal groups have increasingly devoted themselves to thisactivity making this type of service increasingly accessible to anyone. In 2023, we witnessed a new extortion tactic, where the malicious actor threatens to report the victim through legal proceedings, after he has been committedand has not reported to the competent authorities.

Engineering Social

Social engineering was the most prevalent attack technique in 2023. The use of these techniques explores the interest, preoccupation, curiosity and fear of people, mainly through email, to obtain confidential information such as access credentials. This is the preferred technique for cybercriminals for initial access to organisations' internal networks. Unfortunately, many emails with malicious content, especially URLs, still go through basic email filters and end up being sent to users.

Dos/DDoS

DDoS is one of the most impacting cyber threats, causing services unavailability or diminishing their performance. In 2023, the use of Botnets or even the growth of DDoS-for-Hire servicesincreased the number of denial-of-service attacks as well as their volumetrics. This year, the largest DDoS attack on record was reported, targeting Google's services.

Attempt from Login

Due to the resistance to the use of the dual authentication factor, the login attempt remained one of the most common attacks in 2023. Attempts to log in/attacks of brute force use the trial and error technique toadd the victim's login information. Malicious actors use all possible combinations to gain access to the account in question.

4,

What we saw in.PT in 2023

CHAPTER 4

Main Indicators

164
Events Reported
(public channel)

647
Cases DNS Abuse: identified

89 %
Cases DNS Abuse:

Phishing

8 % ~330k
Emails malicious received

130
Cases DNS Abuse: reported

82 %
Cases DNS Abuse mitigated
(less than 8 days)

Implementation Standards Security in Registrars

Web

22.9 %

Registrars with DNSSEC on the page

94.3 %

Registrars with Certificate Digital Valid on Page

94.3 %

Registrars with HTTPS on the Page

85.7 %

Registrars with HTTPS Redirect on Page

35.3 %

Registrars with HSTS on Page

2.9 %

Registrars with

The PTSOC – Security Operations Center of.PT – conducted a study on the implementation of the main security standards in the web and email aspects in the platforms provided by Registrars.PT.

Implementation Standards Security in Registrars

Dane on the Page

Implementation Standards Security in Registrars

Email

14.3 %

Registrars with DNSSEC in E-mail

85.7 %

68.6 %

Registers with DKIM in Email

62.9 %

Registrars with DMARC in E-mail

Webcheck

20.9 %

Web pages tested with DNSSEC

81.007

Tests realised

71.2 %

Web pages tested with HTTPS

8.1 %

Web pages tested with HSTS

50.2 %

E-mail tested with SPF

44.5 %

•fr

E-mail tested with

Training & Awareness

5

Courses cybersecurity

3239

People impacted

7

Editions of PTSOC {Digest}

4

Editions of PTSOC {News}

16

Workshops PTSOC

673

People impacted

Training available

MOOC “Risk Management” cybersecurity in organisations»

MOOC "Management of Continuity

CHAPTER 5

5

Where to look in 2024

Ransomware—as-a-service (RAAS) has become a business ..

Ransomware is one of the most lucrative cyberattacks of the moment. In 2024, the RaaS model will continue to grow continuously as it has proven to be an incredibly efficient vehicle to maximise profits from ransomware attacks. Although the growth trajectory remains the same, the main target of ransom-ware attacks does not. The involvement of governments, government and security entities in the defense of critical infrastructure will motivate ransomware groups to target small and medium-sized enterprises.

Where to look in 2024

“The Advent of the attacks through Supply Chain»

Attackers always seek reliable connections that allow them to gain access to the target’s networks causing as little noise as possible.

Supply Chain attacks occur when attackers infiltrate systems through a partner or service provider with privileged access to the target’s networks.

This will be one of the main attack vectors expected for 2024, being one of the topics to be addressed by key organisations with the entry into force of diplomas such as the NIS 2.

Where to look in 2024

“Engineering social indistinguishable e

Social engineering is one of the most difficult security problems to solve because no compliance, governance or risk management action can solve the fact that people are imperfect and susceptible to being deceived.

Access to Artificial Intelligence and Machine Learning technologies for audio and video manipulation will make it easy to create content so realistic that it will be increasingly difficult to distinguish from reality.

Strengthening Awareness campaigns in organisations will be key, yet more means will be needed to limit the impact of these attacks using Zero Trust principles.

References

1 | Cybersecurity Observatory, Risks and Conflict Report 2023 https://www.cncs.gov.pt/docs/rel-riscosconflitos2023-obcibercncs.pdf

2 | ENISA Threat Landscape 2023
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

3 | significant Cyber Incidents
https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

4 | Dan GOODIN, Ransomware group reports victim it breached to SEC regulators https://arstechnica.com/security/2023/11/ransomware-group-reports-victim-it-breached-to-sec-regulators/

5 | Google
https://cloud.google.com/blog/products/identity-security/goole-cloud-mitigated-largest-ddos-attack-peaking-above-398-million-rps

.pt

Production: January 2024 Grafism: .pt