Annual Report PTSOC 2023

"The Ransomware year"

Index

CHAPTER 1

1.

Overview

In 2023, in a global context in which cybersecurity incidents and cybercrime continue to increase in number and sophistication, with ransomware, online scams and social engineering techniques such as phishing, smshing and more recently quishing, with the use of QRCodes, leading the cyberspace threat landscape. These techniques, amplified by advances in Artificial Intelligence (AI) and machine-learning (ML), will allow analyzing and processing large volumes of data, in real time, automating and introducing greater sophistication in these types of attacks.

This trend is reinforced in the World Economic Forum's Global Risks Report 2023, which anticipates the generalization of cybercrime and cyber insecurity as two of the top 10 global risks in the coming years and elevates cyber(in)security as one of the main issues to address by the European Community in the agenda of the EU's Digital Decade 2030.

This PTSOC annual report aims to present a summary of the main events and trends that were observed in 2023 in the areas of cybersecurity and put into perspective the main challenges that lie ahead for 2024.

CHAPTER 2

2.

Grandes ciberataques de 2023

January

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

February

The **Super Bock** group was the target of a **ransomware** cyberattack that caused constraints in the **supply** operations of some of its products on the commercial market.

March

The **French National Assembly's** website was the target of a **DDoS attack** by a group of pro-Russian hackers, **becoming temporarily unavailable**.

April

Samsung employees unintentionally **exposed internal code and internal meeting notes** when using **OpenAI's 'ChatGPT'** tool to help them identify errors and produce meeting summaries.

May

The **Polytechnic Institute of Leiria** suffered a cyberattack that left 14,000 students without internet access in schools and residences. This attack ended up causing instability in its services, namely the **unavailability of all the institution's online activity**.

June

GlobalCaja, based in the Spanish city of Albacete, was the target of a cyberattack (Ransomware) that **blocked several offices and exfiltrated confidential data, client and employee documents, passports, and contracts**. The Play ransomware group claimed responsibility for the attack.

July

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

August

Several Italian banks suffered DDoS attacks. The national cybersecurity agency in Italy confirmed that at least five Italian banking entities were targets of cyberattacks. **With these attacks, the websites of these banking entities became unavailable, making them inaccessible**. The pro-Russian group NoName was identified by Italian authorities as having been the malicious actors responsible for these attacks.

Septembre

The municipality of Gondomar, on September 27th, was the target of a cyberattack, forcing authorities to take systems offline and contact the National Cybersecurity Centre and the Portuguese Data Protection Authority. The Rhysida ransomware gang, which carried out the cyberattack, released passports and financial documents after the ransom was not paid.

October

DNA testing company **23andMe** reported unauthorized access to the biometric data of 5.5 million customers in October. Malicious actors used previously compromised accounts to carry out a "**credential stuffing**" attack. This type of attack could have been avoided by customers by not reusing passwords. This incident also highlighted the need for companies to proactively analyze the security of their users' accounts.

November

The North American multinational aerospace and defense development company **Boeing** suffered a cybersecurity incident by the LockBit ransomware gang where around 43 GB of data was published online. The incident posed no threat to aircraft or aviation security.

December

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

CHAPTER 3

3.

Main cyber threats of 2023

Ransomware

The year of 2023 was marked by the growth in the provision of Ransomware-as-a-Service (RaaS) services. This business model has become particularly profitable and cybercriminal groups have increasingly dedicated themselves to this activity, making this type of services increasingly accessible to anyone. In 2023, we witnessed a new extortion tactic, where the malicious actor threatens to report the victim through legal measures, after the victim has been compromised and has not reported it to the competent authorities.

Social Engineering

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

DoS/DDoS

DDoS is one of the most impactful cyber threats, causing services to be unavailable or decreasing their performance. In 2023, the use of Botnets or even the growth of DDoS-for-Hire services increased the number of denial-of-service attacks as well as their volume. Also, this year, the largest DDoS attack was reported, targeting Google services.

Login Attempt

Due to resistance to the use of double-factor authentication, login attempts continued to be one of the most common attacks in 2023. Login attempts/brute force attacks use trial and error to guess the victim's login information. Malicious actors use every possible combination to gain access to the account in question.

CHAPTER 4

What we saw at .PT in 2023

Key Indicators

164
Reported events
(public channel)

8% ~330k
Malicious emails
received

647
DNS Abuse:
identified cases

130
DNS Abuse:
reported cases

89%
DNS Abuse:
Phishing Cases

82%
DNS Abuse:
mitigated cases
(less than 8 days)

Security Standards Implementation in Registrars

Web

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

22.9%
Registrars with DNSSEC

94.3%
Registrars with Valid Digital Certificate

94.3%
Registrars with HTTPS

85.7%
Registrars with HTTPS Redirect

35.3%
Registrars with HSTS

2.9%
Registrars with DANE

Security Standards Implementation in Registrars

E-mail

14.3%
Registrars with DNSSEC

85.7%
Registrars with SPF

68.6%
Registrars with DKIM

62.9%
Registrars with DMARC

Webcheck

20.9% ↑
Web pages tested with DNSSEC

81.007
Tests

71.2% ↑
Web pages tested with HTTPS

8.1% ↓
Web pages tested with HSTS

50.2% ↑
Email tested with SPF

44.5% ↑
Email tested with STARTTLS

Training and Awareness

5
Cybersecurity courses

3239
People reached

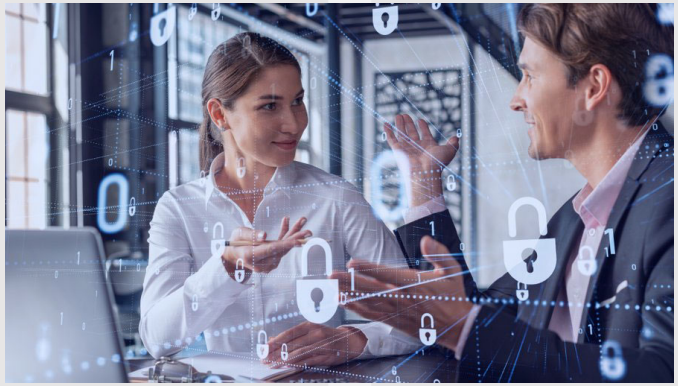
7
PTSOC {Digest} editions

4
PTSOC {News} editions

16
PTSOC Workshops

673
People reached

Training available



[Mooc “Cybersecurity Risk Management in Organizations”]

[Mooc “Business Continuity Management”]

CHAPTER 5

5.

Predictions for 2024

"Ransomware-as-a-service(RaaS) has become a thriving business"

Ransomware is one of the most profitable cyberattacks of the moment. In 2024, the RaaS model will continue to see continued growth as it has proven to be an incredibly efficient vehicle for maximizing profits resulting from ransomware-type attacks. While the growth trajectory remains the same, the primary target of ransomware attacks does not. The involvement of governments and of government and security entities in the defense of critical infrastructure will motivate ransomware groups to target small and medium-sized businesses.

Predictions for 2024

“The advent of attacks through the Supply Chain”

Attackers always look for trustful connections that allow them to gain access to targets' networks while causing as little noise as possible.

Supply Chain attacks occur when attackers infiltrate in 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 that will have to be addressed by essential organizations with the entry into force of directives such as NIS 2.

Predictions for 2024

"Social engineering indistinguishable from reality"

Social engineering is one of the most difficult security problems to solve because any compliance or risk management action can solve the fact that people are imperfect and susceptible to be deceived.

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

The reinforcement of Awareness campaigns in organizations will be fundamental, however, it will be necessary to implement more means to limit the impact of these attacks using Zero Trust principles.

References

1 | Observatório de Cibersegurança, Relatório Riscos e Conflitos de 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

ptsoc

January 2024
Graphic Design: .pt