PTSOC 2020 Annual Report

“Cyberpandemic’s year”

Index

CHAPTER 1

1

Context

In 2020, in response to the covid-19 pandemic context, the future came faster and a true digital revolution took place, through the massive adoption of technology and online to overcome a wide range of fundamental demands arising from the crisis. Digital made it possible to maintain activities and ensure the most basic needs, thus mitigating the devastating economic and social consequences of the pandemic.

It is more than ever agreed that the Internet is a vital resource and that the life of modern societies depends on technology. However, it is important to recognize that the digital world is vulnerable and carries risks. Risks that were amplified in 2020, with a very significant increase in malicious activity in cyberspace, which needs to be monitored.

This first report by the .PT Security Operations Center - PTSOC - presents a brief summary of the main events and trends that we observed in 2020 in the domains of cybersecurity, providing greater knowledge to address the challenges ahead of 2021.

CHAPTER 2

2

2020 Biggest Cyber-Attacks

January

Travelex, a British currency exchange network that carries out 150 million transactions per year worldwide, was the target of a ransomware cyberattack and was forced to suspend its activity, taking its sites offline in 30 countries.

February

A software error on the Danish Finance Portal exposed personal information for 1.26 million Danes, that is, one fifth of the total population in Denmark. This vulnerability has been exposed for 5 years (from 2015 to 2020), until it was discovered.

March

The Marriot hotel chain, in April, was the target of a cyber-attack, having been used by hackers with internal user credentials to access systems and applications in the hotel chain and to exfiltrate personal information of more than 5 million customers.

April

EDP, the Portuguese energy operator, was the target of a cyber-attack that allowed hackers to filter more than 30 TB of sensitive information from the company.

May

Nine millions. This was the number of EasyJet customers who were exposed to a cyber attack. Faced with these events, EasyJet faced a £ 18 billion lawsuit.

June

Ransomware. this was the cyber threat that affected the University of California (UCSF) in June and that made it disburse a total of $ 1.14 million to recover its data.

July

Elon Musk, Jeff Bezos, Joe Biden, Barack Obama, Bill Gates. We could be enumerating some of America's most influential personalities. But not. These were the people who, after a phishing attack directed at Twitter, saw their Twitter accounts being controlled by malicious agents.

This attack had, in its first hour, a financial impact of at least $ 118,000.

August

Intel, a famous processor manufacturer, was the target of a Data Breach that included more than 20GB of internal documents classified as confidential.

September

Düsseldorf Hospital was the target of ransomware. This attack made it impossible for the hospital to receive a patient in need of urgent medical care. Consequently, this patient had to be transferred to another hospital, 30km further away. Since the time is critical and crucial in these situations, the patient ended up, unfortunately, dying.

October

The International Maritime Organization, responsible for shipment security and prevention of marine pollution from ships, was the target of a sophisticated cyber attack that forced the organization to shut down its systems, leaving its public services inaccessible.

November

AstraZeneca was the target of a cyber attack in order to steal information about the research carried out within the scope of COVID-19. This cyber attack is believed to have been developed by hackers located in Pyongyang, North Korea. The hackers posing as recruiters on LinkedIn and WhatsApp, sent AstraZeneca employees malicious documents that would give access to the pharmaceutical company's internal systems.

December

SolarWinds, an American network technology company, with customers belonging to the Fortune 500, acknowledged that malware was inserted into software updates on the Orion platform. The active exploitation of this vulnerability led to the 2020 cyber attack, which is certainly one of the most striking in the history of cybersecurity, impacting 18,000 customers, namely FireEye, Microsoft, American government entities, among others..

CHAPTER 3

3.

2020 Top Cyber Threats

Covid related Phishing campains

Associated with the need for access to information about the COVID-19 pandemic, the number of phishing campaigns has skyrocketed. We have seen an increase in phishing in the order of 600%, namely associated with offers of screening tests, financial support due to the crisis or even fraud related to distance education.

Attacks targeting remote workers

2020 was also marked by the mass adoption of technologies that allowed distance work. The introduction of these new technologies has brought new opportunities for organizations, but also new risks. The massive use of the Zoom application was one of the most cited cases with the discovery of vulnerabilities that allowed the remote execution of vulnerabilities (RCE).

Cloud Services

In view of the growing adoption of cloud technologies, several cyber attacks in 2020 showed that cloud services can be compromised through a variety of techniques. Nevertheless, the greatest risk in adopting the Cloud is related to the incorrect configuration of remote accesses to these systems. In 2020, we saw cybercriminals exploiting vulnerabilities, notably associated with the lack of use of multi-factor authentication, to access management tools and thereby control organizations' systems.

Ransomware, the biggest threat

Clearly, 2020 was the year that we saw the most attacks using this modus operandi. The means used are more sophisticated, the ransom requests have become greater and new extortion techniques have started to be tried by cybercriminals.

CHAPTER 4

4

What we saw, within .PT, in 2020

Main Indicators 2020

3
Security
Audits

368
Internally
Events
Reported

Top 3 Threats

DNS Abuse
detected cases – **186**

.PT Zone
Enumeration – **24**

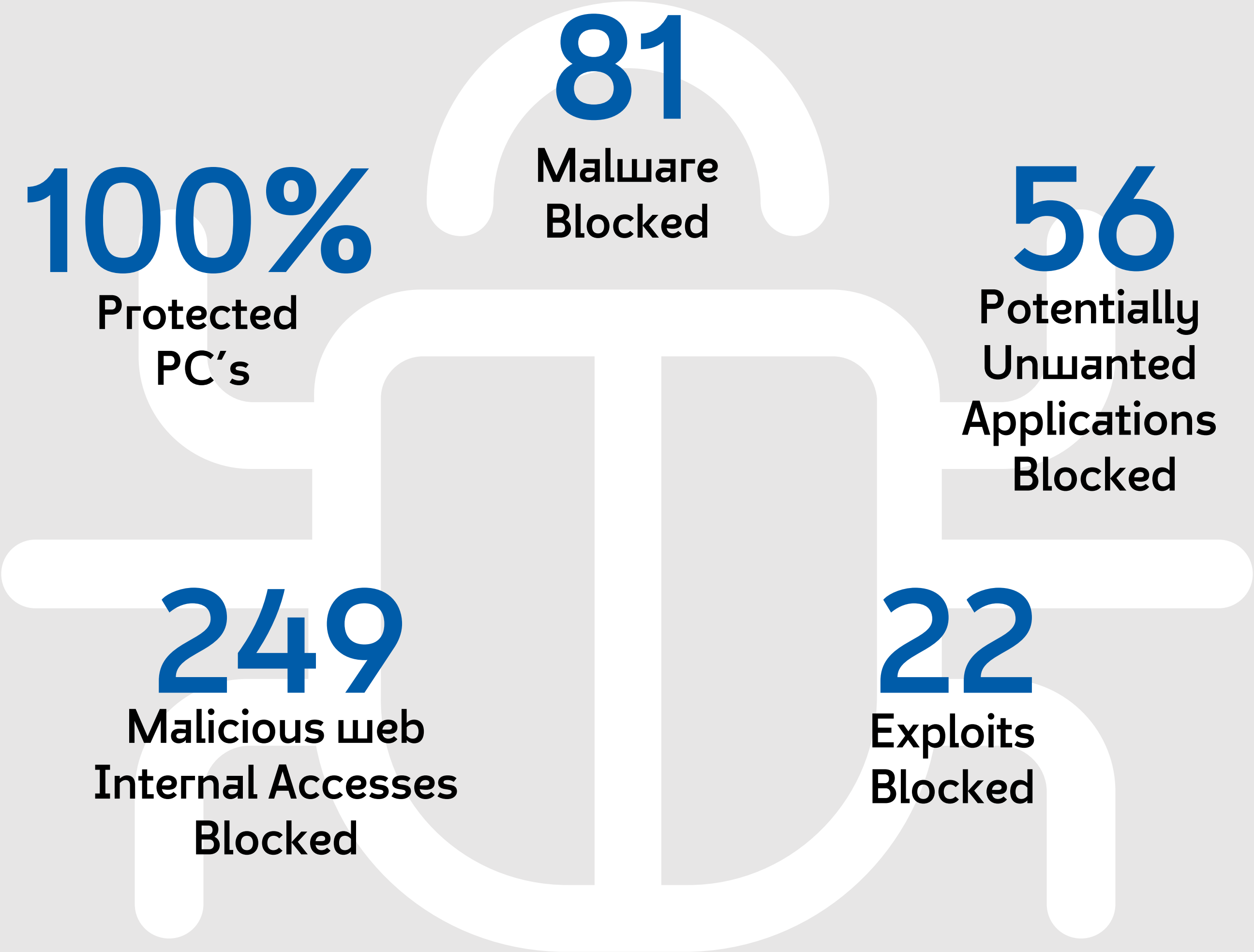
Abnormal
user behaviour – **23**

369
Security Events

123
Events
Rerported
abuse@dns.pt

What we saw, within .PT, in 2020

Malware



81
Malware Blocked

100%
Protected PC's

56
Potentially Unwanted Applications Blocked

249
Malicious web Internal Accesses Blocked

22
Exploits Blocked

What we saw, within .PT, in 2020

Phishing/Spam

645.142
E-mails
Received

2%
E-mails failed
DMARC policy

10.48%
Spam/Malware
E-mails

5%
E-mails failed
DKIM policy

62.57%
Increase number
of emails with malware

61%
E-mails failed
SPF policy

What we saw, within .PT, in 2020

DNS Abuse

64
DNS Abuse cases

28
Phishing

14
Spam

23
Malware

With the revision of the registration rules in .pt, the concept of DNS Abuse was introduced.

A domain name registered in .pt can be classified as DNS Abuse when it supports one or more of the following activities: Malware, Botnets, Phishing, Pharming and Spam.

What we saw, within .PT, in 2020

Webcheck

121
Mean visits
per day

19.644
Tests
realized

66.5%
Web pages
tested with
HTTPS

19.7%
Web pages
tested with
DNSSEC

10.2%
Web pages
with HSTS

47.0%
Email tested
with SPF

29.8%
Web pages
with STARTTLS

What we saw, within .PT, in 2020

Awareness sessions

82.14%

Security Quizz
Mean

3

Awareness
Actions

9

E-mails
of Internal
awareness

CHAPTER 5

5.

Strategy and Cooperation

Assembly of the Republic | In 2020, in cooperation with .PT, efforts were made to implement DNSSEC in Parliament's domains, as well as security measures in its electronic mail were reinforced.

.PT | The .PT partnership with the National Cybersecurity Authority (CNCS) was strengthened with the entry into the Panorama program.

Webcheck.pt | Streamlining the platform that results from the joint initiative of .PT and CNCS, which aims to promote the adoption of good practices and standards that contribute to ensuring security, integrity and confidentiality in internet communications.

.PT | The policy that formally defines how to share the .pt zone file with its partners has been defined and published.

European Union Council (EU) | For the first time, the EU has applied restrictive measures to natural and legal entities following support for carrying out various cyber-attacks on European entities.

European Union Council (UE) | Presentation of the new European cybersecurity strategy and the revision of the NIS Directive (2.0)

CHAPTER 6

6.

Where to look in 2021

> “It is expected that attacks directed at teleworkers will increase both in number and in sophistication”

In 2020, cybercriminals made phishing their main cyberweapon, as a gateway to access organizations' systems and information. In addition to the traditional factors (low cost and ease of implementation), the social context of the pandemic has aggravated the motivation for this practice.

Teleworking is here to stay. In 2021, with the foreseeable extension of the social situation of the pandemic and the measures, more or less, restrictive of confinement, teleworking is expected to continue to be a reality of organizations in guaranteeing their activities.

In this alignment, it is expected that attacks directed at teleworkers will increase both in number and in sophistication.

Where to look in 2021

“The target became the exfiltration of information”

Recent cases of Ransomware illustrate that this activity is highly impactful for organizations and extremely profitable for cybercriminals.

However, in 2020, we began to see a trend of change in the modus operandi of Ransomware attacks, where the target became the exfiltration of information, that is, the theft and consequent ransom request instead of simple encryption and request for ransomware. rescue.

It is thus expected that, in 2021, ransomware and derived activities will continue to be one of the biggest cyber threats to organizations.

Where to look in 2021

> “People have become the new perimeter of organizations”

In response to the context of the Covid-19 pandemic crisis, many organizations had an urgent need to move or take their first steps in the digital world through services provided in the Cloud.

Unfortunately, in addition to the urgency in adopting digital, there has been an increase in vulnerable systems in these environments, mainly due to inadequate security settings.

In 2021, with the pandemic context expected to continue, we will see a significant increase in attacks on Cloud systems. With the increasing adoption of this technology and teleworking, organizations no longer have their traditional physical perimeter. People have become the new perimeter of organizations. Therefore, it will be strategic, in the coming years, to reinforce the activities of identity management and privileged access.

Where to look in 2021

“It is expected that the scale of denial of service (DDoS) attacks will reach records in bandwidth”

The expectation of 5G is high. People want a more connected and more automated future.

Although 5G allows organizations to accelerate their digital transformation and create new experiences in the relationship with customers, for example, the possibility of autonomous driving of vehicles. This technology also increases the attack surface exponentially. We will have more interconnected devices in the digital world, with a much higher bandwidth. Therefore, new cyber risks for organizations appear.

In 2021, it is expected that the scale of denial of service (DDoS) attacks will reach not only records in bandwidth, but also in the number of vulnerable IoT devices exploited by botnets in the digital world.

Quote of the year

“With great flexibility comes great responsibility”

Dennis Okpara, Chief Security Architect & DPO at IDEE GmbH

References

1 | Acronis, Acronis Cyberthreat Report 2020, https://dl.acronis.com/u/rc/WP_Acronis_Cyber_Threats_Report_2020_EN-US_201201.pdf

2 | Observatório de Cibersegurança, Relatório de Cibersegurança em Portugal, Dezembro 2020, https://www.cncs.gov.pt/content/files/relatorio_sociedade2020__observatoriociberseguranca_cncs.pdf

3 | Checkpoint Research, Cybersecurity Report 2020, https://www.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf

4 | TechHQ, Six cybersecurity trends heading our way in 2021, https://techhq.com/2020/12/six-cybersecurity-trends-heading-our-way-in-2021/

5 | Comissão Europeia, Nova Estratégia da UE para a Cibersegurança e novas regras para aumentar a resiliência das entidades críticas físicas e digitais, Dezembro 2020, https://ec.europa.eu/commission/presscorner/detail/pt/ip_20_2391

ptsoc

January 2021
Graphic Design: .pt

.pt