Telefónica

TREND REPORT_

State of Cybersecurity in Spanish companies_

05.10.2017

CYBER SECURED BY ElevenPaths

elevenpaths.com

Index

Executive summary

This study aims to show the state of cybersecurity of both Spanish companies in general and those included in the IBEX 35. The information has been provided by BitSight, which calculates the security ratings of companies based on information external to the organizations themselves. The data set covered by the report includes around 1 000 000 IP addresses allocated to a total of 850 organizations. In view of this context, it can be stated that:

1. "The level of security for Spanish companies is below the European average."
2. "The two IBEX 35 companies with the highest ratings belong to the Financial and Energy / Resources sectors."
3. "Over 85% of IBEX 35 companies are vulnerable to POODLE, Logjam, DROWN and FREAK."
4. "Threats targeting the mobile channel have made their way to the third place in the ranking of the most widespread infections within Spanish companies."
5. "Only 6 IBEX 35 companies did not exhibit any system compromises in the last year."

DO YOU KNOW WHAT IS YOUR ORGANIZATION'S POSITIONING IN FACE OF THESE CHALLENGES?

If you would like to **know your security rating** and compare yourself with your industry, please contact securityrating@11paths.com to receive your report.

1. Introduction

In recent years there has been an exponential development in the field of Information and Communication Technologies (ICT). As a result, ecosystems have become more global and organizations need to be permanently interconnected. At the same time, IT infrastructures are increasing in number and complexity, services are outsourced and business models increasingly depend on suppliers and partners.

This evolution entails **new risks and a potential growing impact** for organizations, since, at the same time, cybercriminals have evolved their tactics and objectives. In this way, all types of organizations, regardless of their size and sector of activity, are subjected to a wide variety of increasingly sophisticated attacks.

It has been a long time since, in 1903, knowledge of what is considered the first leak in history was brought to light. At that time, Southern California Hospital for the Insane suffered the disappearance of records containing personal and medical information about its patients, allegedly stolen by one of the workers [1].

Spain has recently suffered the global attacks of WannaCry [2] and Adylkuzz [3]. Although other attacks with the same notoriety have not spread nationwide, internationally, it is becoming more and more frequent to find news of all types of companies and institutions affected by attacks of various kinds. While the typology of these incidents varies widely, **information leaks** are possibly the **attacks with the greatest impact**. This is due to the fact that the sensitivity of the exposed information and the volume of filtered records is increasing, **reaching an average cost of $ 3.62 million** [4] (which includes both direct and indirect expenses incurred by an organization as a result of an information leak).

While cybercrime figures are on the rise, investment in cybersecurity is keeping pace. According to Gartner's latest forecast, global information security spending would reach $ 93 billion by 2018 [5]. In the case of Spain, the average investment in cybersecurity has risen from $ 3.1 million to $ 3.9 million in the last five years [6].

Are Spanish companies and organizations secure? Are we more or less secure than other countries around us? Is the average increase in security investment sufficient? Do we invest our resources in security efficiently?

At ElevenPaths **we believe that macro knowledge of the country's security** is a clear differential value that allows us, in advance, to support our clients to tackle the particular challenges they face every day.

To this end, we have created this report, which aims to provide an executive overview of the **state of cybersecurity in Spanish companies**.

In order to endow the report with the most relevant information, it will be prepared periodically to be able to analyze trends and advise the organizations where they should focus their attention.

2. Methodology

This report has been prepared in collaboration with BitSight, analyzing information from its security ratings, a system developed to measure the overall level of security of organizations around the world. These ratings, updated daily, rate organizations on a scale of 250 to 900, classifying them in three categories depending on the rating: Basic, Intermediate or Advanced.

Security ratings are calculated using a proprietary algorithm based on information from various risk vectors distributed into the following categories:

- **Compromised Systems:** Refers to the system compromises of the organization, typically caused by malicious software.
- **Diligence:** Observable measures that a company has taken to prevent attacks.
- **Employee Behavior:** Looks for user file sharing activity that can introduce malicious software into an organization, for example, by downloading a compromised file.
- **Data Breaches:** Refers to publicly disclosed incidents of data loss or data theft. These include data loss through successful attacks, employee negligence and hardware theft.

It is important to note that ratings are derived from **externally observable data** on an organization's security posture.

BitSight collects and processes vast amounts of data in order to provide the security ratings. The foundation of this research is built on the ability to accurately identify security events and attribute them to companies, which in turn, enables aggregation across industries. This attribution is determined by identifying the CIDR (Classless Inter-Domain Routing) blocks, domains, and AS (Autonomous System) numbers that organizations own. The process to build these network maps has shown an accuracy over 95%, even for companies with hundreds of thousands of IP addresses.

In the analysis of the IBEX 35, for those companies that are multinational, their global infrastructure has been taken as a reference, given that it is understood that any incident at a global level has repercussions for the whole company.

3. General overview

According to data provided by BitSight, the cybersecurity level in Spanish companies is **slightly below the European average**. Leading the European ranking are countries such as Germany, the United Kingdom or France (Group A), with a security level in the intermediate range. Portugal and Italy (Group B) are examples of countries whose security level is similar to that of Spanish companies.

Expanding the reach at a global level, it can be seen that European countries lead the security ranking, gaining a certain advantage over the United States of America, Australia and Japan (Group C). On the other hand, Peru, Colombia or Brazil (Group D) would maintain similar levels of security in South America.

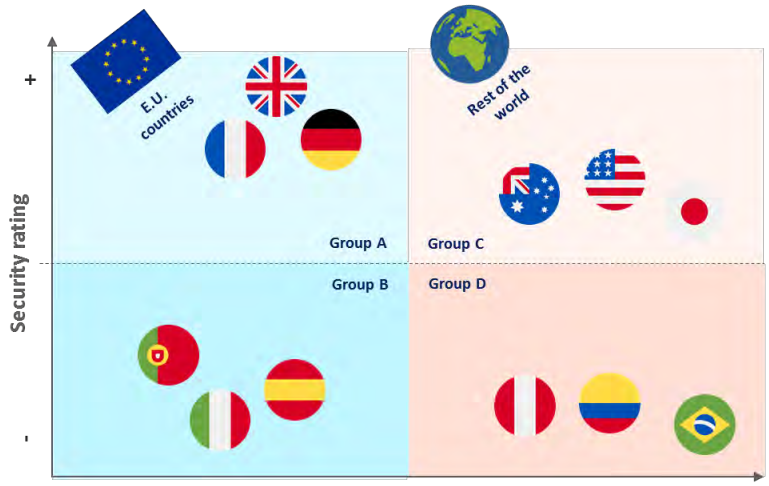

Figure 1. Comparison of the security rating of Spanish companies with other countries

After a general analysis of Spanish companies, the **most widespread types of infection** are **botnets** (Conficker, AndroidBauts, Nivdort, ZeroAccess, and Necurs) and **potentially unwanted applications** (CrossRider, Sprotect, Grayware, and Genieo). The "Spam Bot" type represents an unidentified infection that results in the massive sending of spam.

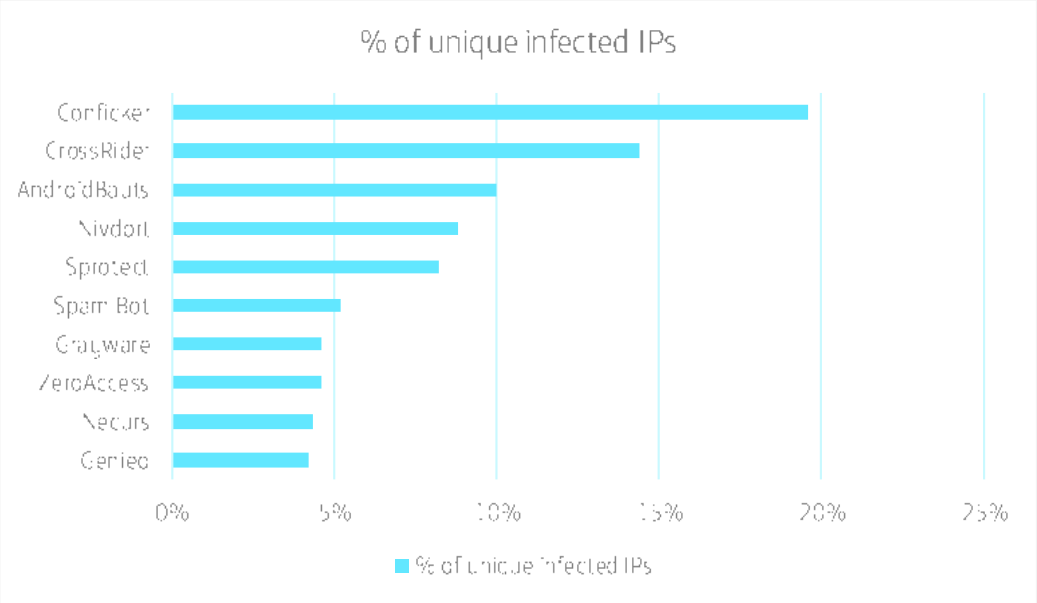

Figure 2. Top infections in the last 30 days in Spanish companies

In the case of vulnerabilities, those registered in the last 30 days are related to **TLS/SSL deficient configurations** (Logjam, POODLE, DROWN, FREAK, Heartbleed, Ticketbleed) or **server configurations** (DOUBLEPULSAR, CVE-2017-0144, CVE-2017-7269), as in the past year, according to the "Vulnerability trends of the first half of 2016" report.

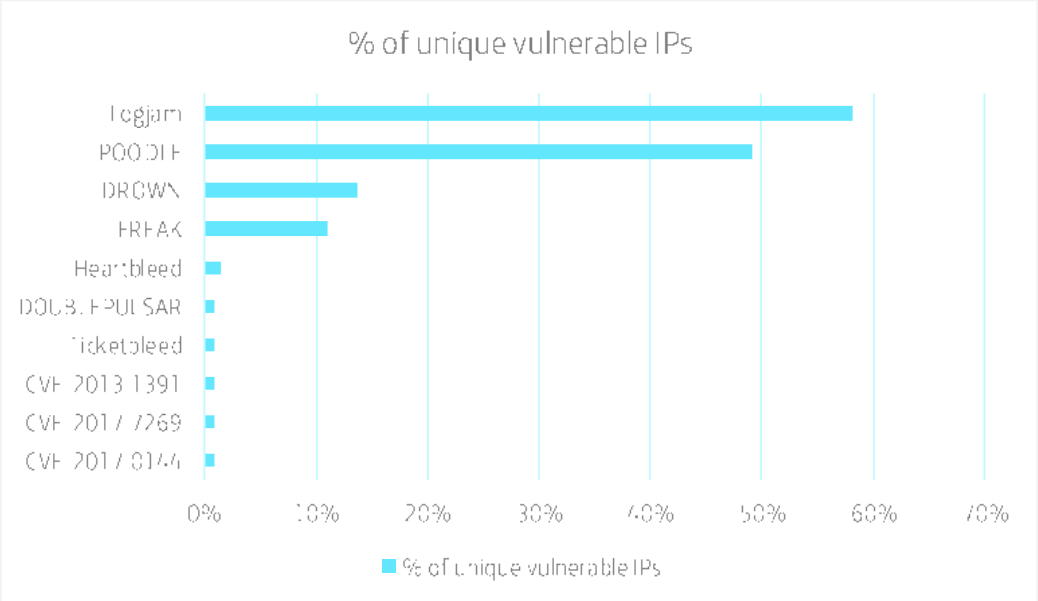

Figure 3. Top vulnerabilities in the last 30 days in Spanish companies

With regard to open ports, ports are identified running services like **SMTP without STARTTLS**, **FTP without STARTTLS** and **Telnet**, which undoubtedly poses a security risk.

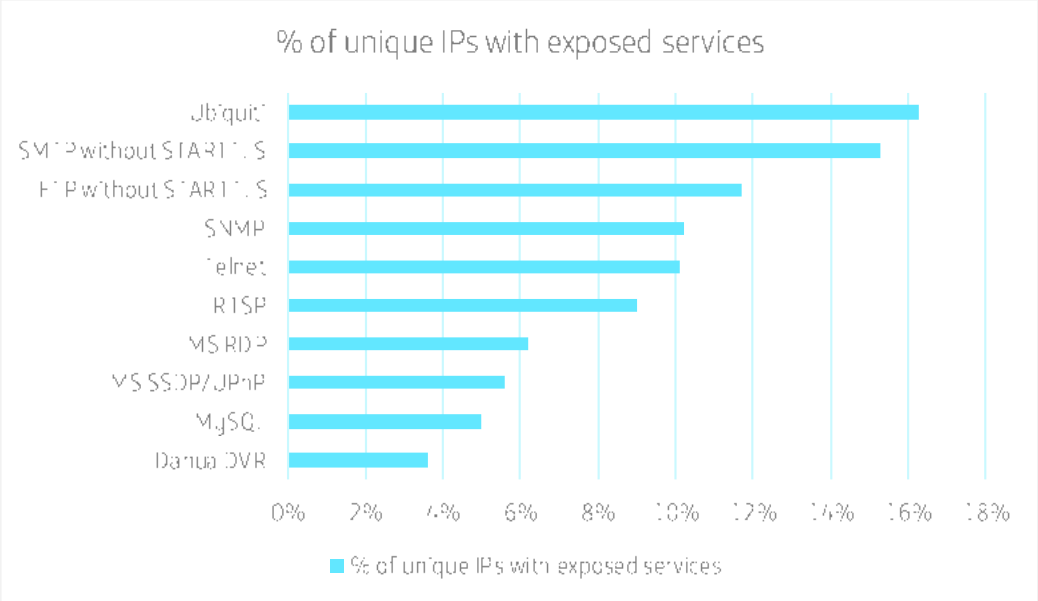

Figure 4. Top open ports with exposed services in the last 30 days in Spanish companies

Up to this point, the report has provided a global view of risk in Spanish companies. To further contextualize this picture, it has been decided to focus on a set of companies that generate significant business volume and are critical to the country's economy, and even to the supply chain of other organizations. The IBEX 35, the reference stock market index of the Spanish stock exchange, has been chosen for this purpose.

Since the B2B sector of large companies holds an important place within ElevenPaths, this choice is intended to present conclusions that are as relevant as possible for our customers.

Therefore, from now on, the report will focus on analyzing the security posture of IBEX 35 companies.

4. Compromised systems

Most incidents detected in the IBEX 35 are related to infections of devices through malicious software, commonly known as malware.

Risks from malware infections can result in **business continuity disruption** and increased risk of **data breaches**. Hence the importance of assessing compromised systems in organizations. In this sense, it can be seen that the most common infections among IBEX 35 companies over the last year are:

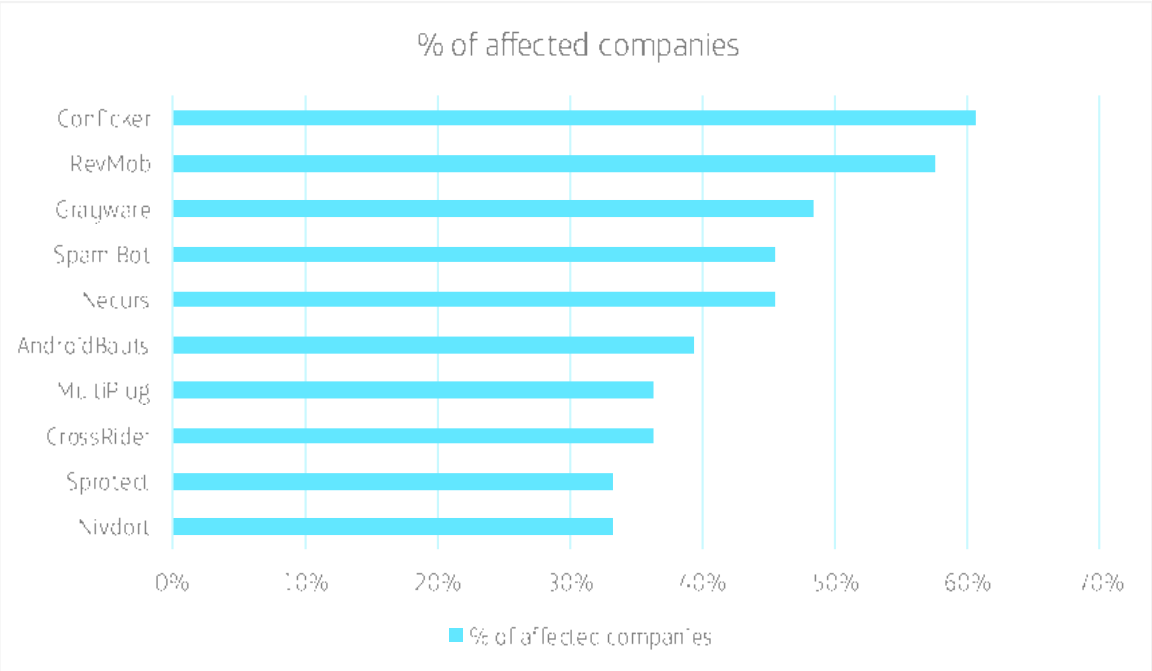

Figure 5. Top infections in the IBEX 35 over the last year

On an individual level, of all these infections, Conficker and AndroidBauts stand out. Both are known botnets, with different repercussions and methods of infection.

In the case of Conficker, it spreads through a vulnerability in the Windows Server service or infected USB drives, and its main objective is to steal information from the infected device and carry out mass mailing campaigns. It is particularly significant that it continues to be so widespread across so many sectors, since in 2008 Microsoft released an update that fixes the vulnerability used to spread. This shows that the **pace at which companies patch known vulnerabilities is not** always **the most convenient** to avoid this type of situations.

AndroidBauts infections occur through malicious applications installed from official and non-official markets, and are mainly aimed at displaying ads, in addition to stealing information from the phone that allows the installation of third-party applications. The arrival in the top 10, as well as the presence in more than half of the sectors, of this **malware especially targeted at Android mobile devices**, reflects the increasingly important dimension that is acquiring the use of the mobile channel in companies and the risks involved.

Significant insight can also be obtained by focusing on sectors. For example, the presence of Spam Bot, an unidentified type of infection that results in the massive sending of spam, is observed in 68.7% of the sectors. This data is important given that some of these **sectors (Financial, Energy / Resources)** are customer-oriented and **could be generating phishing campaigns against them** for their own customers.

Having a look at the most important sectors in the IBEX 35, in terms of the total number of companies, the Financial sector also shows other infections with a large presence: Necurs and Grayware affect more than 65% of the organizations; and CrossRider and Conficker affect half of the sector. However, there is also more positive view of the data. For example, the presence of Zeus, a malware family that has been one of the biggest threats to the financial sector worldwide for nearly ten years, is reduced to one third of the organizations.

On the other hand, in the Energy / Resources sector, half of the companies are affected by RevMob and Conficker. While in the Utilities sector, Grayware affects 50% of companies.

In general, as shown, the **most common types of infection are botnets** (Conficker, Necurs, AndroidBauts and Nivdort) **and potentially unwanted applications** (RevMob, Grayware, MultiPlug, CrossRider and Sprotect).

In the case of botnets, infected devices may be participating as bots or Command & Control (C&C) servers on a huge network of infected computers that are dedicated to performing DDoS, sending spam, distributing malware, or mining cryptocurrencies.

Meanwhile, potentially unwanted applications are usually adware or spyware that installs additional unwanted software, modifies a browser's home page or search provider, injects advertising or performs other actions without the user's consent.

5. Vulnerabilities

The above-mentioned problem of known and unpatched vulnerabilities is common to all sectors. However, it is not the only problem facing organizations nowadays.

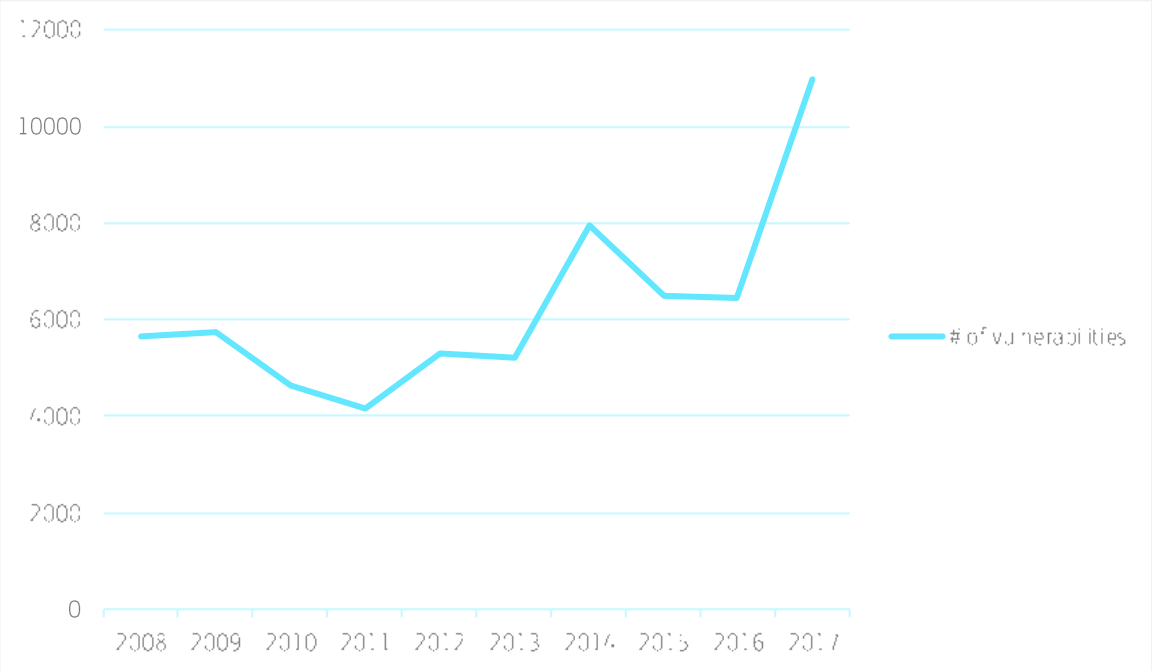

Figure 6. Evolution of the number of vulnerabilities published in the last ten years

Analyzing the evolution of the number of vulnerabilities in the last ten years [7], it is particularly significant the increase in this year compared to last year. If the trend continues, **the number of vulnerabilities could double before the end of the year.**

Among all these vulnerabilities, the most representative in the IBEX 35 are those listed in Figure 7:

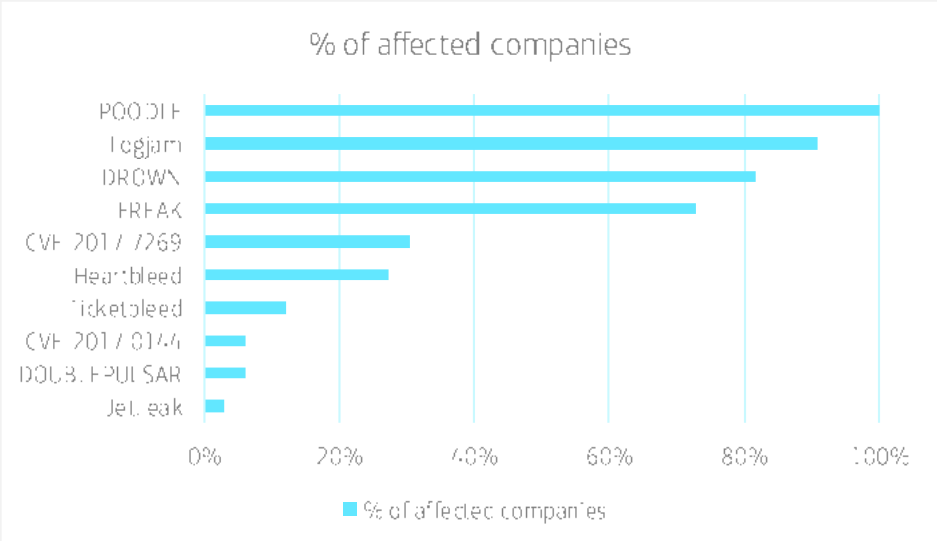

Figure 7. Top vulnerabilities in the IBEX 35 companies over the last year

More than 85% of IBEX 35 companies are affected by the 4 most widespread vulnerabilities (**POODLE, Logjam, DROWN and FREAK**). These cryptographic vulnerabilities allow extracting unencrypted data by Man-in-the-Middle (MitM) attacks, and decrypting encrypted data transmitted over TLS.

It is also interesting to see how **DOUBLEPULSAR**, which was used as a backdoor to install WannaCry ransomware, **is still present in two IBEX 35 companies** despite the fact that Microsoft released a security patch months ago to fix the vulnerability.

However, the most significant data obtained after analyzing each of the **vulnerabilities** that make up this top 10 is that **70% are public** for more than a year, even reaching three years in some cases. This highlights the **lack of updated patching policies**

In addition, the severity of these vulnerabilities, according to the Common Vulnerability Scoring System (CVSS) standard, in its version 3.0, is High or Critical in at least half of the cases. And there are public exploits for 60% of them.

6. Open ports

While there are certain ports that must be open to support business functions, others, are unnecessary. And when they run vulnerable services, they become a perfect entry vector for cybercriminals.

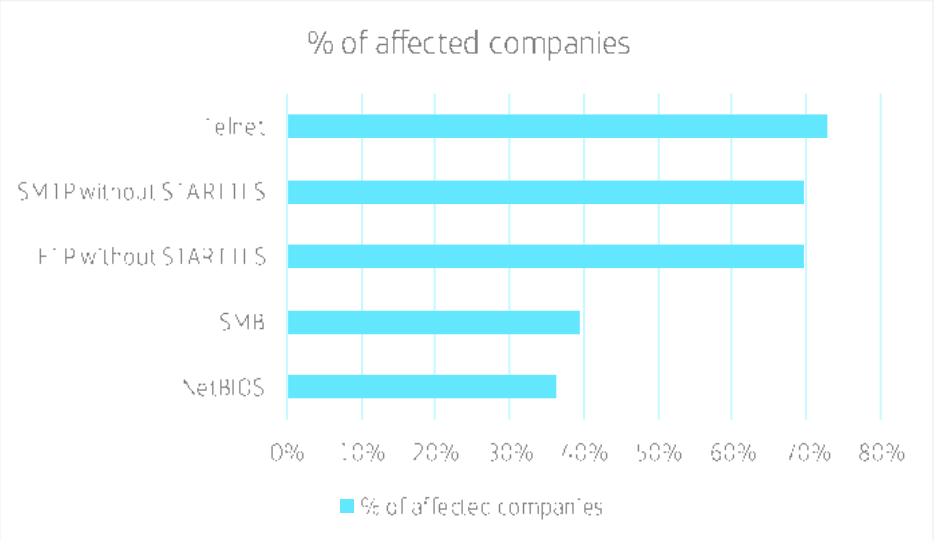

Figure 8. Top open ports with the most critical exposed services in the IBEX 35 over the last year

Among these 5 services, which have been selected as the most critical of all those observed, Telnet deserves a separate mention. Its presence in almost three-quarters of the IBEX 35, covering more than 80% of the sectors, is worrying. It is a communication protocol that does not encrypt traffic and has known vulnerabilities, which should be replaced, as much as possible, by SSH.

Other fairly common communication protocols (SMTP and FTP) have been found running unencrypted versions in a large number of sectors (13 and 14, respectively), resulting in a perfect entry vector for malware, in addition to the risks inherent to the lack of encryption.

SMB, famous for being used by DOUBLEPULSAR, is a protocol that, inadequately configured, allows access to shared folders, and has been found in almost 40% of companies.

Finally, it is noteworthy that NetBIOS continues to be used in 12 companies belonging to more than half of the IBEX 35 sectors. It is true that certain legacy applications still depend on its use, but it has known vulnerabilities and is subject to many attacks.

Furthermore, it should also be noted that **popular database servers** such as MySQL (very widespread in all sectors, being present in 15 companies) **are still remotely accessible due to erroneous configurations.**

7. Recommendations

Despite the fact that most organizations currently have numerous security solutions in place, many have infections or vulnerabilities and exposed services, so they could be victims of advanced cyberattacks. It is therefore necessary to take a series of recommendations into account to prevent these incidents or mitigate their impact, if they occur.

First of all, it is important to emphasize that organizations need to consolidate the basics of security in order to grow on a solid foundation and protect themselves against more advanced threats. Aligning information security as part of the corporate risk management model, defining and updating security procedures, updating the asset inventory or establishing effective communication mechanisms with IT teams remain the pillars on which the corporate information security policy of large companies should be based. Simplifying: "**Security must be in the company's DNA.**"

Regarding open vulnerabilities and ports, **vulnerability management** needs to evolve beyond a simple scheduled exercise that runs a few times a year, becoming a **continuous process that proactively identifies problems**. To provide an updated picture of the asset inventory, continuously analyze vulnerabilities affecting IT assets and have tools to centralize the life cycle of vulnerabilities. This has become the basis for holistic and efficient management of the vulnerabilities affecting an organization. It is also necessary to make the company's management bodies aware of the impact on the business that a security error would cause, facilitating the creation of efficient communication mechanisms between the CISO and CIO roles, which allow vulnerabilities to be resolved and managed quickly.

Under compromised systems, it is observed that most infections could be prevented or resolved by **establishing basic IT policy measures**. However, it should be noted that this report is based on data from detected events, but there are other incidents that go unnoticed by the conventional defenses of many organizations. **To be prepared for more sophisticated attacks**, organizations are recommended to install **malware detection and response** (EDR) tools that allow them to include next-generation malware detection capabilities and integrate **high-value external IoCs**, as well as facilitate incident response, providing CSIRT teams with context information on the threats that have affected them.

As far as the mobile channel is concerned, the data collected in the report indicates an **increase in malware families** specifically **targeting mobile devices** (AndroidBauts, for example). On the other hand, ElevenPaths' own sources indicate that, among the applications found in the different markets, which already reach over eight million, more than five million contain vulnerabilities, being critical in more than one million of them. Faced with this reality, two lines of recommendation open up: on the one hand, the reinforcement of all security policies around the use of mobile devices in corporate environments, to **protect access to sensitive corporate information**. On the other hand, the use of solutions that allow the **identification of security flaws in their own applications**, as well as the detection of third-party applications that may put organizations or their customers at risk.

8. Bibliography

[1] «Oldest Data Loss Incident – Contest Winners», DataLossDB. 31-may-2009. [En línea]. Disponible en: https://blog.datalossdb.org/2009/05/31/oldest-data-loss-incident-contest-winners/. [Accedido: 19-sep-2017].

[2] F. Palazuelos. «How the WannaCry ransomware attack affected businesses in Spain». EL PAÍS. 19-may-2017. [En línea]. Disponible en: https://elpais.com/elpais/2017/05/19/inenglish/1495181037_355318.html. [Accedido. 19-sep-2017].

[3] Alexander Chiu, «Cisco Coverage for Adylkuzz, Uiwix, and EternalRocks». Talos Intelligence Blog, 22-may-2017. [En línea]. Disponible en: http://blog.talosintelligence.com/2017/05/adylkuzz-uiwix-eternalrocks.html. [Accedido. 19-sep-2017].

[4] «Ponemon Institute's 2017 Cost of Data Breach Study: Global Overview», 19-jun-2017. [En línea]. Disponible en: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&. [Accedido: 19-sep-2017].

[5] «Gartner Says Worldwide Information Security Spending Will Grow 7 Percent to Reach $86.4 Billion in 2017». [En línea]. Disponible en: //www.gartner.com/newsroom/id/3784965. [Accedido. 19-sep-2017].

[6] «Encuesta Mundial sobre ciberseguridad 2017». PwC. [En línea]. Disponible en: https://www.pwc.es/es/digital/encuesta-mundial-estado-seguridad-informacion-2017.html. [Accedido. 19-sep-2017].

[7] «Browse cve vulnerabilities by date». [En línea]. Disponible en: https://www.cvedetails.com/browse-by-date.php. [Accedido: 19-sep-2017].".

About ElevenPaths

At ElevenPaths, Telefónica's Cybersecurity unit, we believe in the idea of challenging the current state of security, an attribute that must always be present in technology. We're always redefining the relationship between security and people, with the aim of creating innovative security products which can transform the concept of security, thus keeping us one step ahead of attackers, who are increasingly present in our digital life.

More information

www.elevenpaths.com
@ElevenPaths
blog.elevenpaths.com

About BitSight

BitSight is transforming how companies manage information security risk with objective, verifiable and actionable security ratings. Founded in 2011, the company built its Security Rating Platform to continuously analyze vast amounts of external data on security issues and behaviors in order to help organizations manage third party risk, underwrite cyber insurance policies, benchmark performance, conduct M&A due diligence and assess aggregate risk. Seven of the top 10 cyber insurers, 100 Fortune 500 companies, and 3 of the top 5 investment banks rely on BitSight to manage cyber risks.

More information

www.bitsighttech.com
@BitSight
blog.bitsighttech.com