Telefónica

TREND REPORT_

Global Banking Cyber report

In collaboration with:

etisalat | SoftBank | Singtel

CYBER SECURED BY ElevenPaths

elevenpaths.com

Table of contents

1. Executive summary

As the world becomes digital, new opportunities and threats arise.

This report aims to give an overview of some of the digital threats for one of the most trusted and important industries – the **banking** industry.

As we keep growing digitally, we tend to focus more on business. This means that when we are trying to develop a new product, website or application among others, we tend to prioritize speed, convenience and ease of implementation **instead of security**.

This report tackles what we consider three key important and often forgotten aspects of security:

- The **security** embedded **in mobile applications**
- The **metadata** available **on public documents**
- The **information** we can obtain **about the services' communications and their quality** (This is, ports opened in servers, their vulnerabilities, etc.).

The results obtained can give us information such as the mobile app developer and find out if this developer works with other companies (and if he/she may be reusing not optimized code for the banking app, or even find out "hidden" and usually more unsecured services).

These three aspects of security are known as *peripheral* security compared to the more traditional security such as access controls, servers hardening...

We will attempt to shed some light on these issues.

2. Introduction

We have conducted a global study with the objective of determining the level of maturity of the security controls in **banks' mobile applications** and the **metadata contained in public files**. This report has been made to assess how banks are protecting their mobile applications, the prevention of metadata information leaks and the devices/hosts exposed on the Internet.

The analysis is based on public files, web and mobile applications of **56 of the biggest banks worldwide**. Additionally we have researched the top two banks from some of the most important countries across all the continents/regions. This aims to give an overview on what banks are doing in each region regarding their online customer-facing services.

We have analyzed the bank's official application using two tools developed and owned by one of the members of the Alliance, to assess what vulnerabilities each application has and provide a vulnerability score. Additionally, we have investigated what permissions each app asks for and which, if any, is the relation among them.

To see the metadata on files, we have utilized public documents detected in the bank domains, which can be accessed by any network user through search engines or directly on the different bank's websites.

The study was focused on obtaining information from public sources. No attempt was made to access private nor confidential documents at any given time. Nevertheless, all information that could potentially help identifying a bank and its vulnerabilities has been blurred out (or erased) and filtered to avoid that potential attackers could use it to carry out a malicious action against the financial companies.

In this report, the information is compiled from three main sources:

- **FOCA OpenSource**, a free tool to find documents through search engines. Once the documents are downloaded, FOCA extracts the metadata contained in the files and then analyses it.

- **Tacyt** and **mASAPP**, two own developed tools that focuses on finding mobile applications vulnerabilities among many other functionalities.

- **Censys** (They define themselves as "Security driven by data"), a public search engine for servers and devices exposed to the Internet. Censys also allows finding specific hosts and services associated to the bank domains we provided and see how websites and certificates are configured.

3. Methodology

The first stage consisted on determining how many banks to analyze and from which countries. We wanted to give a security view of the banking industry worldwide. Therefore, we decided to breakdown the world in seven regions (Asia, Middle East, North America, South America, Europe, Africa and Oceania).

We went on to select the top countries for each region – the amount of countries selected depended on the region (2 for Oceania and North America; 5 for Europe, Africa, Asia, South America; 4 for the Middle East). **28 countries** in total.

We chose two well-established banks in each country, a total of **56 banks** worldwide.

We used **Tacyt** and **mASAPP** tools to analyze the **most updated official application** of each bank. We have only addressed mobile apps for **Android**.

Tacyt helped us on:

- Making comparisons among the apps in terms of number of **permissions** required and their specific characteristics.
- Getting the total amounts of official apps of each bank currently available on Google Play.

- To get these results, we checked the main official app of the bank to get its associated developer name and executed this query (changing <DeveloperName> for the actual developer's name registered):

  developerName:" *<DeveloperName>*" -deadDate:* origin:GooglePlay categoryName:Finance

- This query only looks at one developer's apps (the one that made the main app). The most frequent scenario is to have only one, but a bank can have many different developers for its different official apps. We tried additional different queries customized and adapted to each bank, to get results that are more precise.
- Afterwards we used **mASAPP** to analyze each mobile app to obtain the overall security score, vulnerabilities and risky behavior.
- We also searched for unofficial apps related with each bank. This was harder to do because each uploader can change any of the original parameters (title, developer name, category, etc.) and make it harder to find.
- We used many different queries for each case but we started every time with this one (changing <Name keywords> for each bank's name keywords):

(<Name keywords>) AND (-deadDate:* AND -origin:GooglePlay –origin:AppleStore)

We had to remove some clauses like categoryName:Finance because we found that many apps were re-uploaded to unofficial markets without some information.

For the metadata analysis, we used **FOCA**. **FOCA** allows us to find the digital documents publicly exposed by the banks domains. Once they all are detected, **FOCA** downloads these documents and extracts their metadata.

By extracting the metadata, it is possible to get information like user names, IP addresses, email addresses, network names, storage directories and operating systems. From this information, it is possible to infer unsafe processes or bad practices from the perspective of the information security (use of generic users, obsolete operating systems, emails exposed to credential leaks, emails from non-official domains in official documents, etc.).

Finally, using **Censys**, we found any host related to each bank's official domain. Censys has a domain search engine that shows an enormous amount of information related to each result (information related with each open port as well as additional attributes like IP address, location, etc.) in form of "result attributes".

If we insert a company domain (domain.com) into the Censys' search bar:

- It looks for **partial** matches of this input in all the result attributes and returns the hosts as a result.
- **Except** in one: For Port 443: ***443.https.tls.certificate.parsed.names***, it only shows the hosts as a new result if the searched value matches **exactly** with one of those contained. For example, if the attribute *443.https.tls.certificate.parsed.names* of a host has the values "www.domain.com" or "mail.domain.com" and we inserted "domain.com" in the search bar, it **will not** consider it an exact match and it will not be taken as a valid result. As we want to get partial matches in every attribute, we added "*443.https.tls.certificate.parsed.names:domain.com*" to the query and joined the search conditions with an *OR*.

To remove those results including the domain, **but not** related with the bank, we dropped those that only had matches in its http body. These results usually were non-related sites that mentioned the bank or **did not have** any relation with its official website. Therefore, we added *NOT 80.http.get.body: <Company Domain>* to the query with an *AND*.

The final query to get the closest results to what we want is:

(<Company Domain> OR 443.https.tls.certificate.parsed.names: <Company Domain>) AND (NOT 80.http.get.body: <Company Domain>)

We opted to show results including **Akamai**. In case Akamai results were not considered relevant, we just would need to add "*AND NOT Akamai*" at the end of the query.

This initial query served our purposes to give us an overview and get these first results present in this report, as using the same query for all the searches, we expect to have more coherent results.

Once we collected all the information provided by these tools, we carried out an analysis and determined what information was relevant. We decided to anonymize all these entities and avoid any potential harm to its image.

This whole Methodology can help companies to identify **"hidden" IT assets**.

4. Results

In this section, we provide the results we thought were relevant to show.

4.1. Mobile Applications Analysis and Results

4.1.1. Overall Risk Scoring

Using **mASAPP**, we were able to get a risk score for every single official mobile application. **mASAPP** calculates this score analyzing the type of vulnerabilities present on the application and the number of times these occur within the app.

A score of 0 means that the application has no detectable vulnerabilities and a score of 10 means it is very unsafe. We found that the average score by region was **7.27** (considered a high score for the application). This means that nearly all banking apps have **at least one serious** vulnerability.

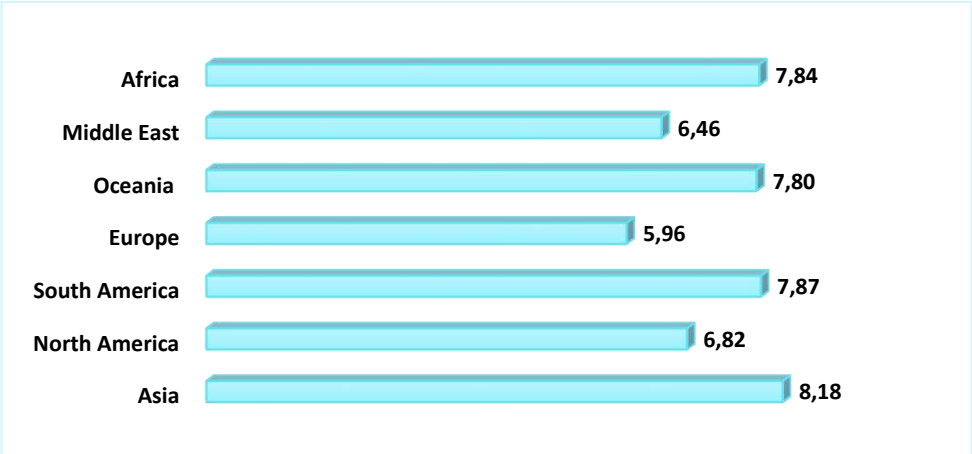

Figure 1. mASAPP – Overall risk score

As seen on the chart above, Asia, Africa and South America have the greatest risks – considered as **High** – while Europe, the Middle East and North America have more of a **Medium** risk score. Not all the analyzed banks in Africa had a mobile application available.

At a very high level, this means that banks in areas where the risk score is higher have more vulnerabilities on average.

Image 1. mASAPP – High-level summary

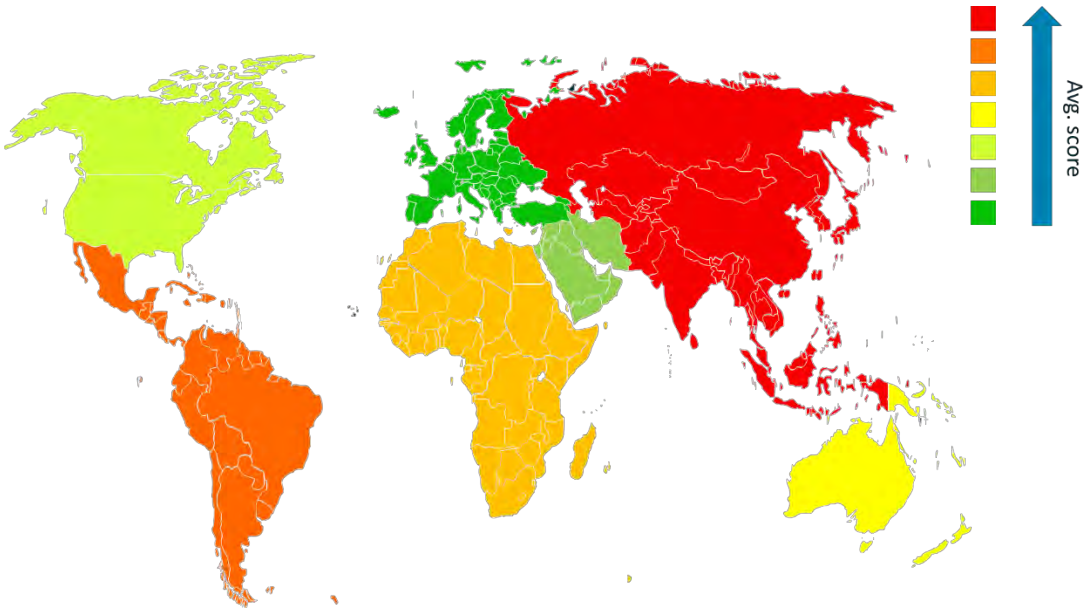

Image 2. mASAPP – Overall risk score per region

4.1.2. Vulnerabilities

The vulnerabilities **mASAPP** can identify include **Code Quality, Improper Platform Usage, Cryptography, Data Storage and Privacy, Network Communication and Reputation** among others.

The most common high-risk vulnerability was the "**Potential SQL Injection Vulnerability**" which was present in **34 out of the 53** applications (56 banks, 3 of them did not have a mobile App).

SQL Injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution. A successful SQL Injection attack could extract customer data (such as credit card numbers) which is extremely important in the banking industry as the mobile applications might carry very sensitive data.

The second most common vulnerability found affected **17 out of the 53** bank applications – roughly a 32% of the banks on the study – and was the "**Insecure Certificate Signature Algorithm**".

In apps with this vulnerability, the application certificate is signed with an **insecure hash algorithm** (such as MD5 or SHA1). This vulnerability could allow attackers to conduct spoofing attacks.

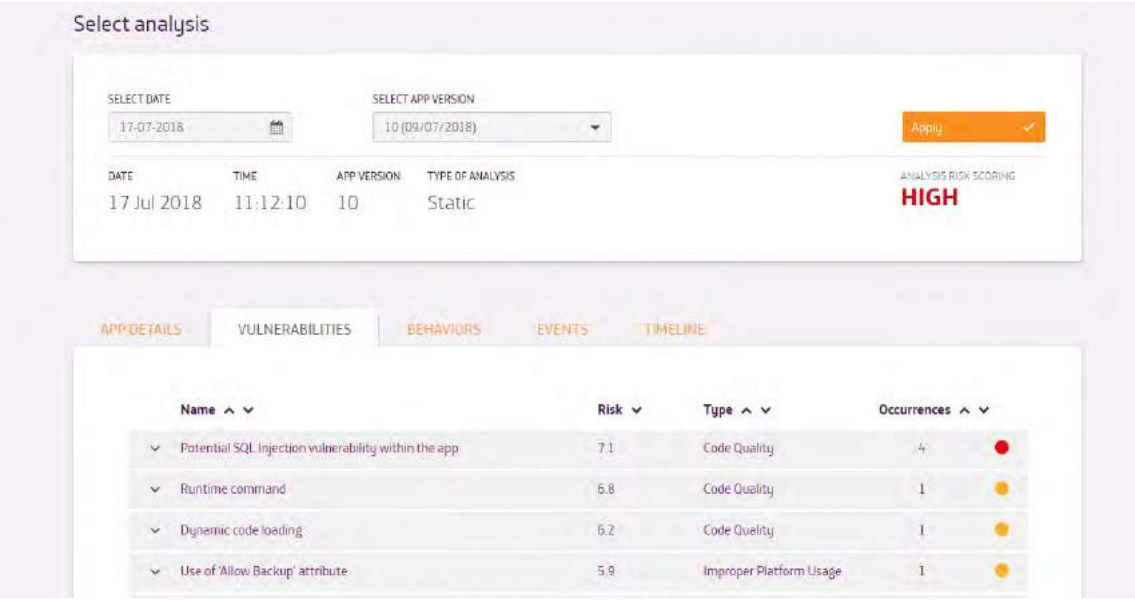

Image 3. mASAPP – Identified Vulnerabilities

Many of the most common vulnerabilities had the root cause in the quality of the code. This might have happened because the teams developing the mobile applications did not follow proper security measures to ensure that the environment was safe but instead focused more on convenience, speed, user interface and/or user usability.

4.1.3. Permissions

The figure below shows the average number of permissions asked by each region.

Middle East banks are the ones asking for less permissions, an average of 15, while banks in Asia tend to ask for more permissions, an average of 23. A difference of 8 permissions on applications from top banks that are supposed to provide in general the same type of services. We ignore if this has anything to do with the different cultures or regulations in each area.

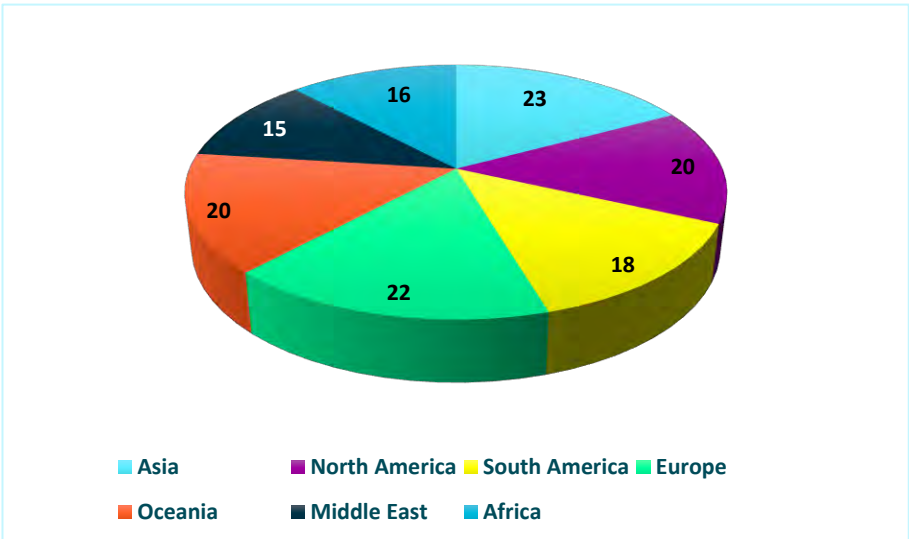

Figure 2. Average permissions required per region

These results lead to the question of how many permissions are **strictly necessary**.

mASAPP highlighted that many of the asked permissions were considered **intrusive**. Intrusive permissions include **system-level permissions** (such as *WRITE_SECURE_SETTINGS*. *INSTALL_PACKAGES*, *CALL_PRIVILEDGED*, etc.).

Besides this, we highlighted some permissions we categorized as **questionable**. Questionable permissions are those we cannot assure that are intrusive or unnecessary (since we do not know exactly all functionalities in each banking app), but we consider that they could be it. Some examples of permissions we considered questionable are:

- **RECORD_AUDIO**: banking apps usually do not have any audio functionalities.
- **CALL_PHONE**: this allows an application to initiate a phone call without going through the dialer user interface for the user to confirm the call. This means, the app can make phone calls without the user pressing the calling button. Banking apps usually do not need to make phone calls but if they have to (for example if the app offers any shortcut to call Customer Support), they should allow the user to confirm the call each time they do it.
- **READ_CALL_LOG and READ_CONTACTS**: user's call log should be irrelevant for the bank and for its apps. Same for user's agenda contacts.
- **READ_SMS**: to allow the app to read SMS makes it able to read all the messages, not only those sent by the bank. The app could analyze messages from the bank in order to get processed information for the user, but it most probably is just an intrusive permission.

Other permissions such as *CAMERA* or *ACCESS_FINE_LOCATION* might look intrusive, but it is important to understand the services provided and how these permissions can improve customer's experience.

- The *CAMERA* permission might be asked due to the feature of accessing the bank account through biometrics.
- *ACCESS_FINE_LOCATION* might be asked because the bank needs to know in which country the user is and understand user's behavior for security reasons (i.e.: Someone may be withdrawing money in Madrid when the user and its mobile phone are in Singapore, which could mean someone is committing a fraud).

mASAPP found many different types of intrusive permissions (*System-level permissions*, *System-level broadcast identified*, *Google dangerous permissions* and *External storage access*) and some Dangerous Features (*Runtime command* and *Dynamic code loading*).

The screenshot below shows the behaviors found by **mASAPP** on a particular banking application.

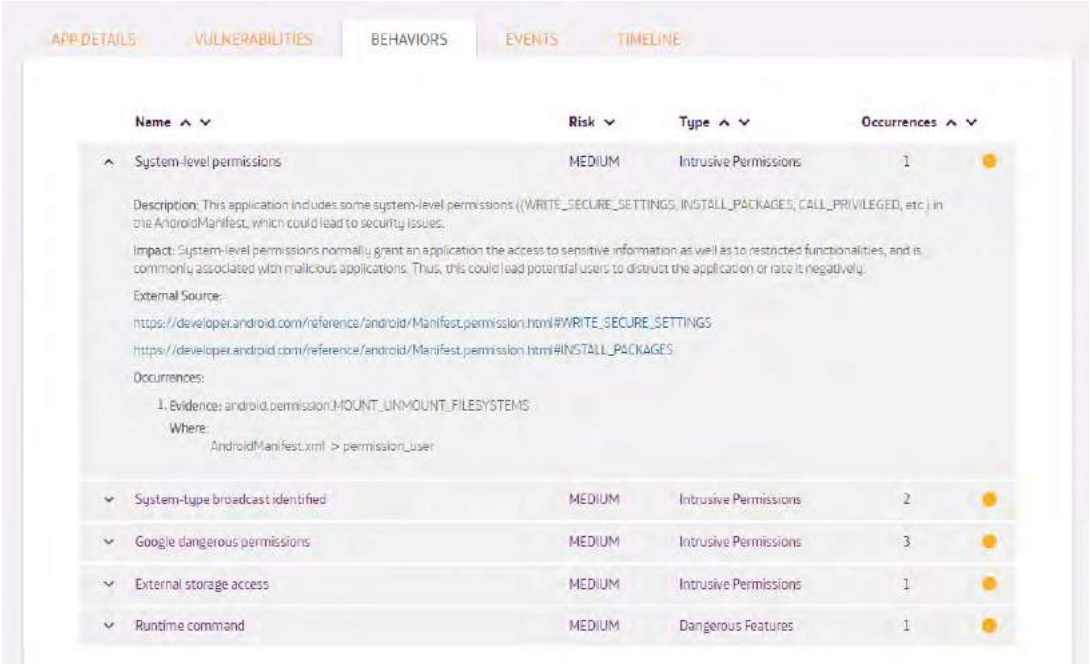

Image 4. mASAPP – Identified Behaviors

We wanted to make a comparison on permissions asked by banking apps all over the world to see if they were consistent. What we found was that although the average permissions asked were of 19, there was **only 1 permission common to all the banking apps – Permission to Internet access**.

This changes when we try to find common permissions per region. In this scenario, we find more permissions that are common: from 1 in Africa (*INTERNET*) to 7 in Oceania (*VIBRATE*, *INTERNET*, *com.google.android.c2dm.permission.RECEIVE*, *WAKE_LOCK*, *ACCESS_NETWORK_STATE*, *ACCESS_FINE_LOCATION* and *USE_FINGERPRINT*).

We used **Tacyt** for these comparisons. We focused on what permissions were requested but **Tacyt** provides many other data comparisons as shown in the screenshots below.

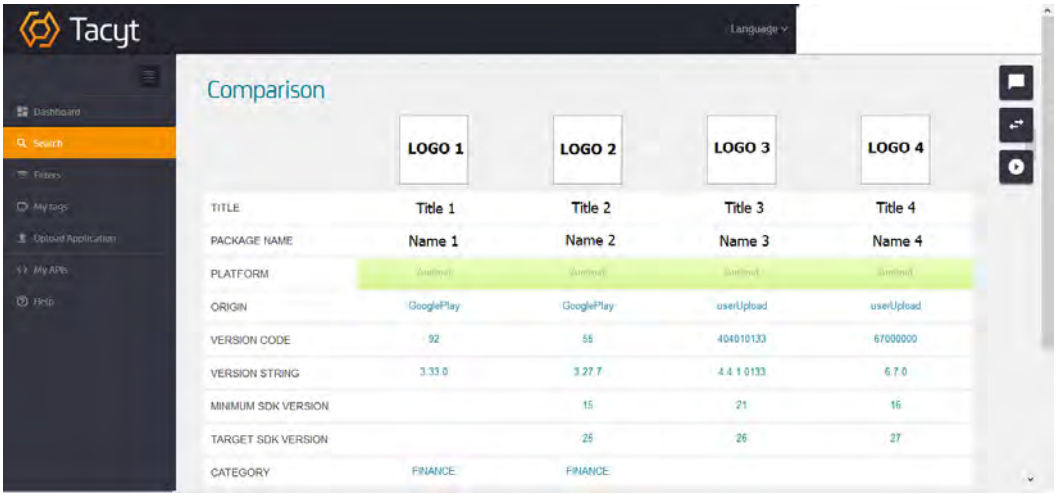

Image 5. Tacyt – Comparison Dashboard

Image 6.Tacyt – Comparison Categories

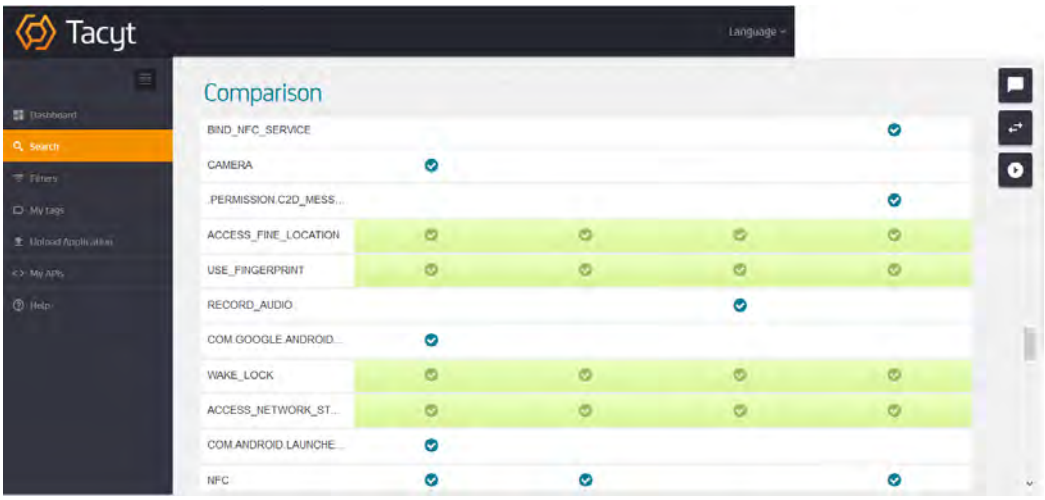

Image 7. Tacyt – Permissions Comparison

4.1.4. Average applications in Google Play official market

Using **Tacyt**, we have identified the number of official bank applications uploaded to Google Play. The more apps available, the more opportunities for a potential malicious actor to attack the bank.

- The **global average** number of applications per bank is **4**.
- **Africa** has the **lowest average** per region: **2** applications.
- **Europe** has the **highest average** per region: **11** official apps.

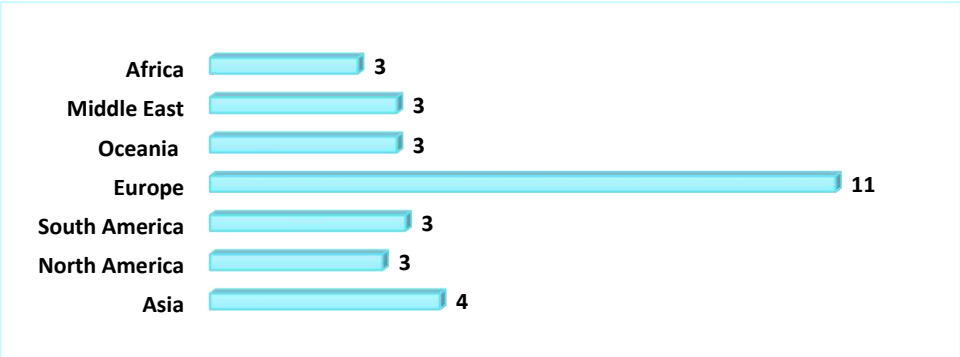

Figure 3. Tacyt -Average number of official applications per region in Google Play

4.1.5 Average applications in unofficial markets.

We searched in eight different unofficial markets: **aptoide**, **mobogenie**, **nineApps**, **SlideMe**, **mobile9**, **1Mobile**, **apkpure** and **a2zapk**.

The next figure shows the average results per region:

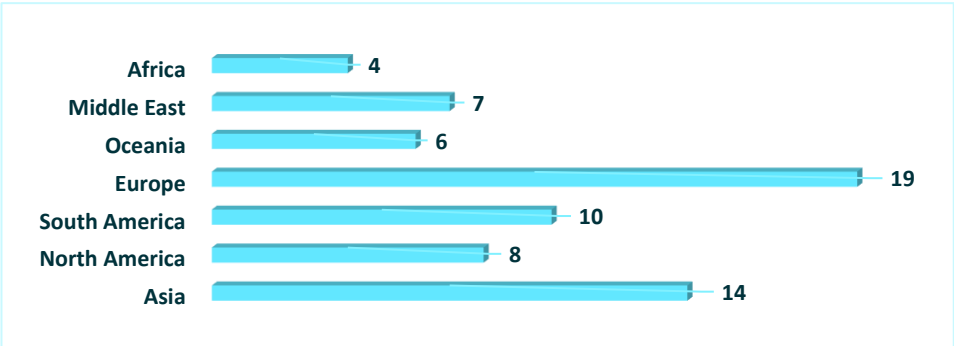

Figure 4. Tacyt - Average number of applications per region in the main non-official markets

- The **global average** number of applications per bank is **10**.
- **Africa** has the **lowest average** per region: **4** applications.
- **Europe** has the **highest average** per region: **19** non-official apps.

- **Asia** is the region with less app-uploading control. Their number of unofficial apps is **3.5 times** their number of official apps.
- Individually, the bank with most unofficial apps uploaded had **49**.
- All of the analyzed banks had at least one app uploaded to an unofficial market.

4.2. Metadata Analysis - FOCA

Using **FOCA OpenSource** (https://www.elevenpaths.com/labstools/foca/index.html) we carried out an analysis on the banks domains. This analysis provided us information like how many documents are public, what type of documents are they, operating systems, software used, user's names and details, etc. On this section, we will point out the most relevant findings.

4.2.1. Initial Analysis

We configured **FOCA** so that it could carry out an automatic search of the main 22 file extensions using Google, Bing and Exalead API keys, allowing them to find the links to those files and downloading them.

In Figure 6, you will find the quantity of analyzed documents per region (4 banks in Oceania and North America; 10 banks in Europe, Africa and Asia, South America; and 8 banks in the Middle East).

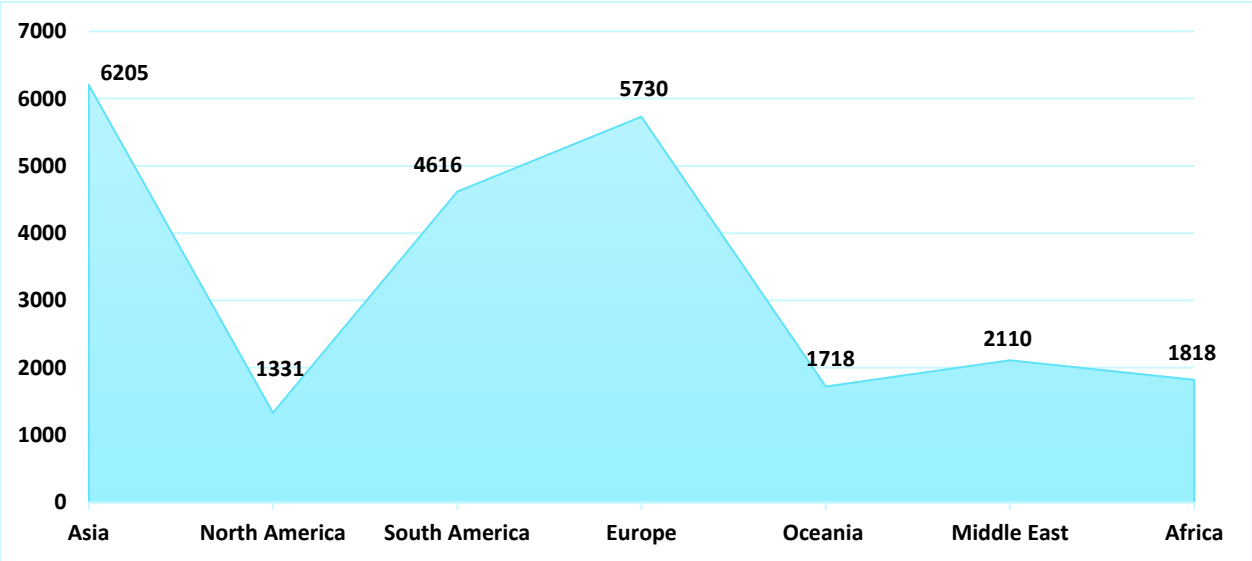

Figure 5. FOCA -Total analyzed files per region

We identified that **the majority of the files** (75% of them) **were PDF documents** followed by unidentified extension documents (8%), Word processors (8%), Spreadsheets (7%) and Presentations (1%) as can be seen on the figure below.

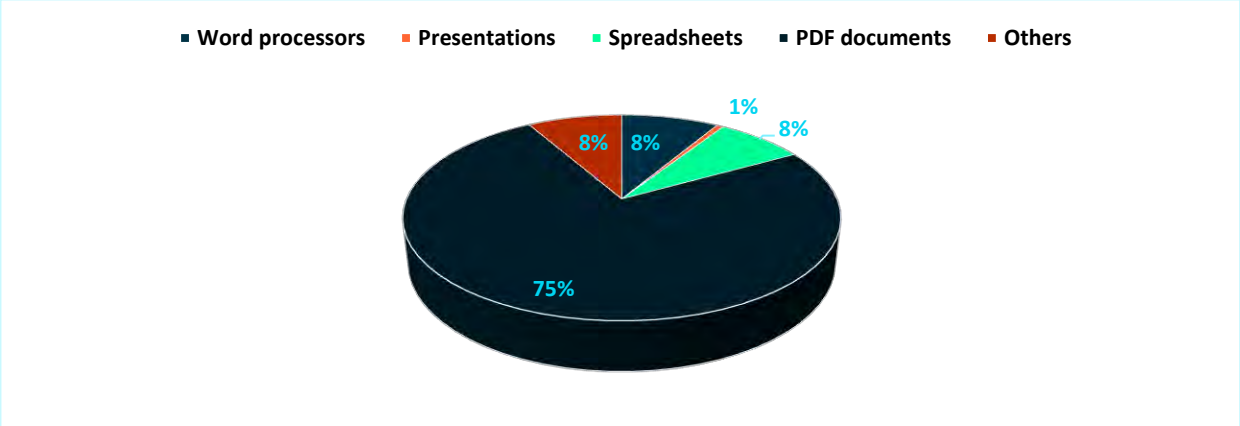

Figure 6. FOCA – Percentage of files extensions analyzed

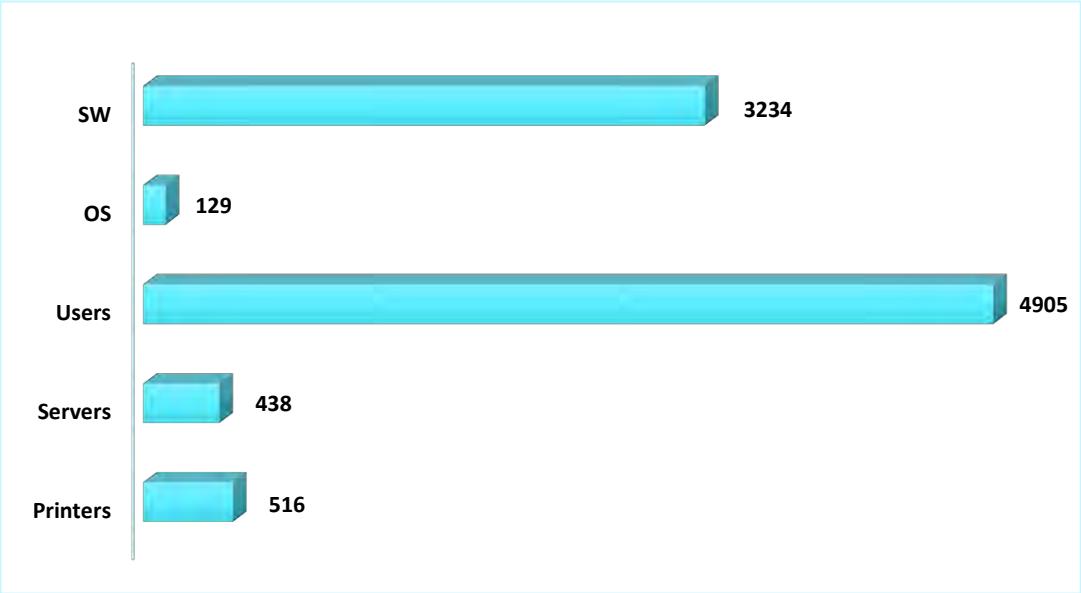

Figure 7. FOCA – Important parameters extracted with amounts

The most frequently used software are **Adobe programs** like Acrobat, Acrobat Distiller, InDesign or PDF Library **and different Microsoft Office versions** (XP, 2000, 2007, etc.). This makes sense since the files we found are mainly PDFs (Adobe), word-processing documents (Word from Microsoft Office), spreadsheet files (Excel from Microsoft Office) and presentation files (PowerPoint from Microsoft Office).

4.2.2. System Analysis

The metadata offers very valuable information used in computer forensic investigations to identify the device where the document was made or to determine a timeline.

However, it also allows a computing criminal to outline the characteristics of the computer or company that he/she wants to attack, reducing the options and improving the effectiveness of the attack.

4.2.2.1. Operating systems

About **10 different operating systems** were found deployed on **2759 computers** – approximately 65% were identified in Asia. The next figure shows the number of operating systems detected in each of the domains analyzed per region.

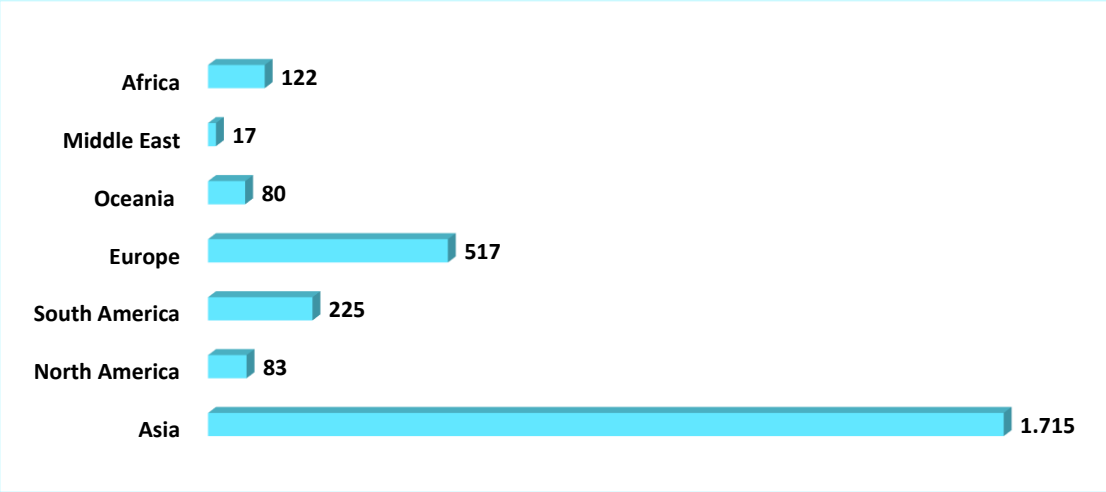

Figure 8. FOCA – Number of computer OS metadata found per region

Since a few years, the most commonly used operating systems are no longer supported by their manufacturers. This generates a critical risk to the information they possess **assuming that the equipment with which those documents were made is still available**.

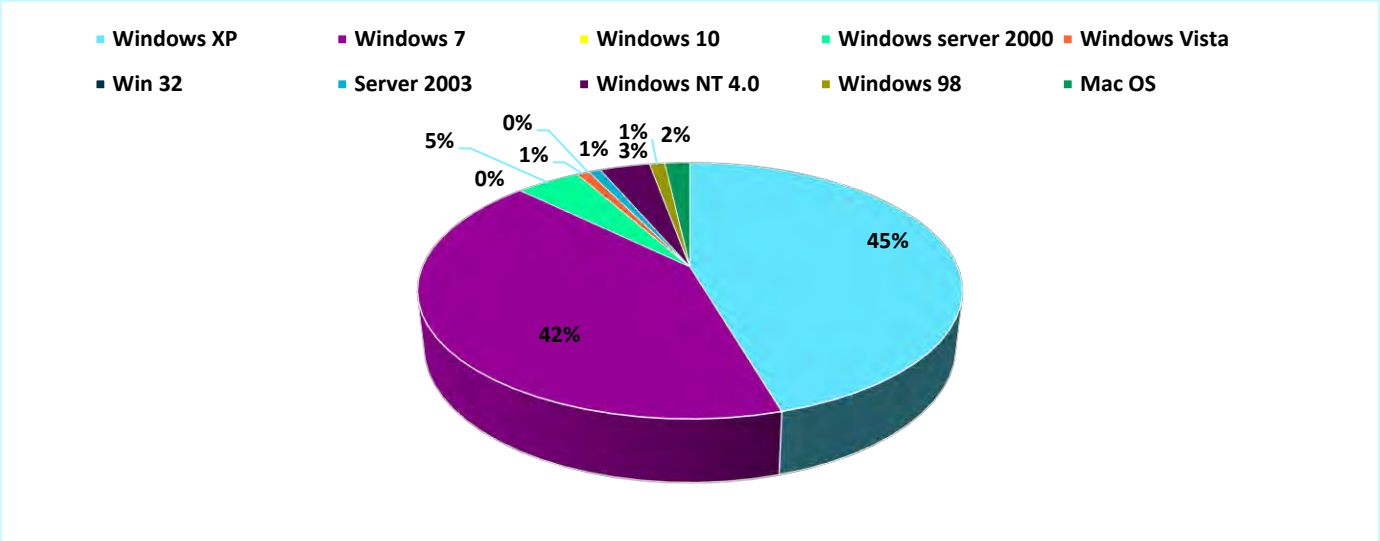

Figure 9. FOCA – OS Overall Ratio

The case of Windows XP (found in nearly half of all computers) is especially relevant. It has not had any security updates nor support from Microsoft since April 2014, so a malicious outsider could exploit this information.

4.2.2.2 Users

The identification of users through metadata allows an attacker to get a list of **valid users within the infrastructure of the organization**. In the analysis process, we found on average 700 users per region with **4905 identified users** in the metadata from the analyzed documents, which were distributed by region as shown in the following figure.

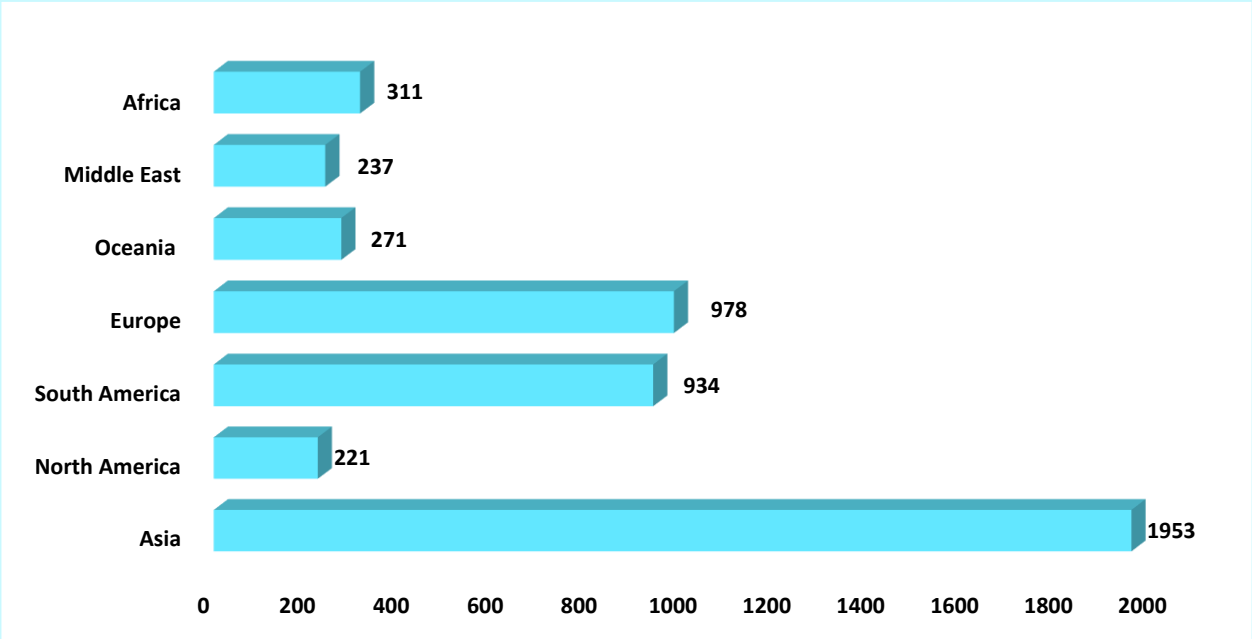

Figure 10. FOCA – Identified users per region

The region that provided us by far the most information from their metadata is Asia. On the low end, we have the Middle East, Oceania and North America.

The use of generic user accounts is a bad practice. This makes it impossible to trace the events within different systems to a specific user, increasing the risk of confidential information loss by a disloyal employee. We found that **most of the banks had at least one generic account**.

We also found **289 admin accounts**, which are supposed to have higher privileges making them a highly appealing target for potential attackers.

4.2.3 Additional interesting information extracted

- We found a user account in Asia called "Any Authorized user" – the use of generic user accounts is a bad practice as explained above.
- Two banks in the same group share official applications and share internal networks – this is a dangerous practice because the vulnerabilities found on one of the applications apply to the other one as well.
- A certain bank in Asia uses open office SW – open office SW is not a good idea since it does not guarantee support nor security.
- Printers in some banks provide too much information (building, floor and internal address) - this information can be useful for potential attackers when doing social engineering for instance.
- We were able to find Human resources related information, which should be internal.
- Having servers allocated in many different countries (because of services like Akamai) is a frequent practice, but some countries known for restrictive measures have 100% of their servers in the same country the bank is located.
- We were able to identify where some servers were physically located. This information should not be public since malicious actors can use it in many different ways.
- A "funny" note is that one bank in Africa names its servers after different animal species such as Wale, Rhyno, etc. This same bank identifies the PC used by the Administrator as "PC_Administrator". This is a very unsafe practice (unless it has been done on purpose as part of a Honeypot).

4.2.4 Overall FOCA Scoring

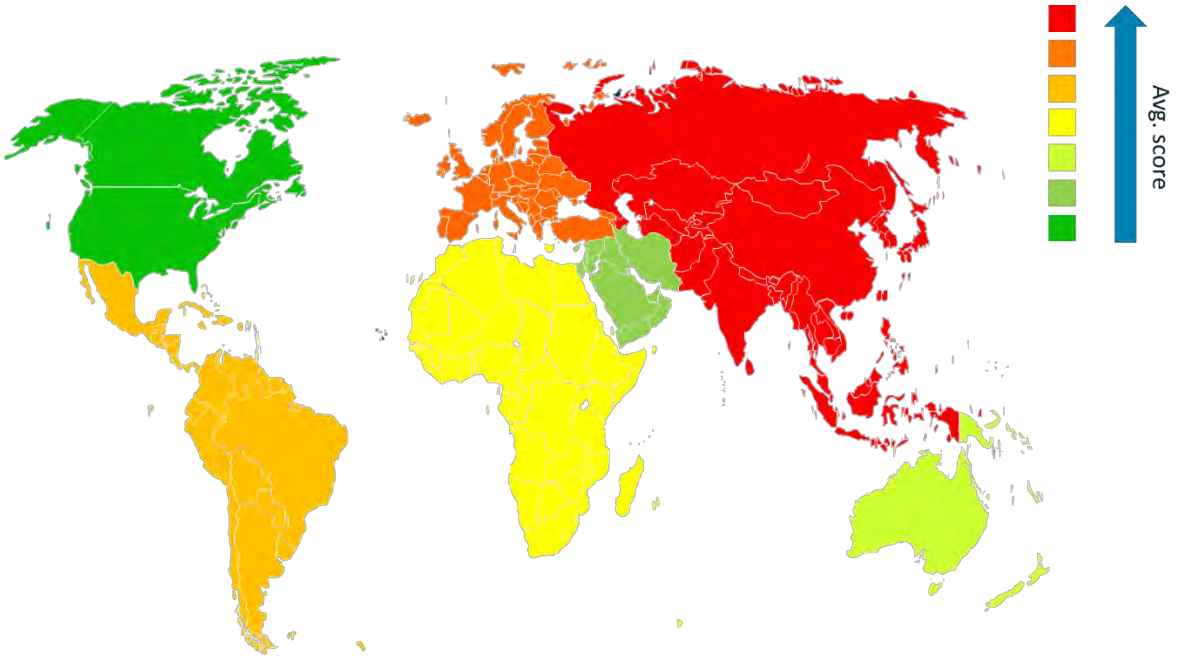

Image 8. FOCA – Overall risk score per region based on available information

We developed a new scoring system based on different parameters obtained from FOCA's results (where a higher the score means FOCA can extract less information).
The graphic above shows that there is not a direct relation between FOCA score and mASAPP score. For example, Europe is the Region with the lowest mASAPP score, but it has the second highest FOCA score.

4.3. Hosts Analysis – Censys

Through Censys.io[1], we were able to see what type of services and protocols were linked to hosts associated to the official bank domains.

An analysis process on the detected services was carried out to determine how many services perform an information traffic assurance using encryption at the connection. The physical location of the server based on the IP address was also analyzed.

4.3.1 Detected Services

As seen on the graph below, **all regions have over 94% of its domains with an HTTPS connection available**. On the other hand, the total average of domains **with HTTP connection available is 67%** - which is relatively important since it is an insecure protocol.

[1] It needs to be mentioned that you can run the query on two different days and the results will vary a bit. A not well-intended person can run Censys.io to find out which new services such as FTPs are available and start launching new attacks over such new spotted services.

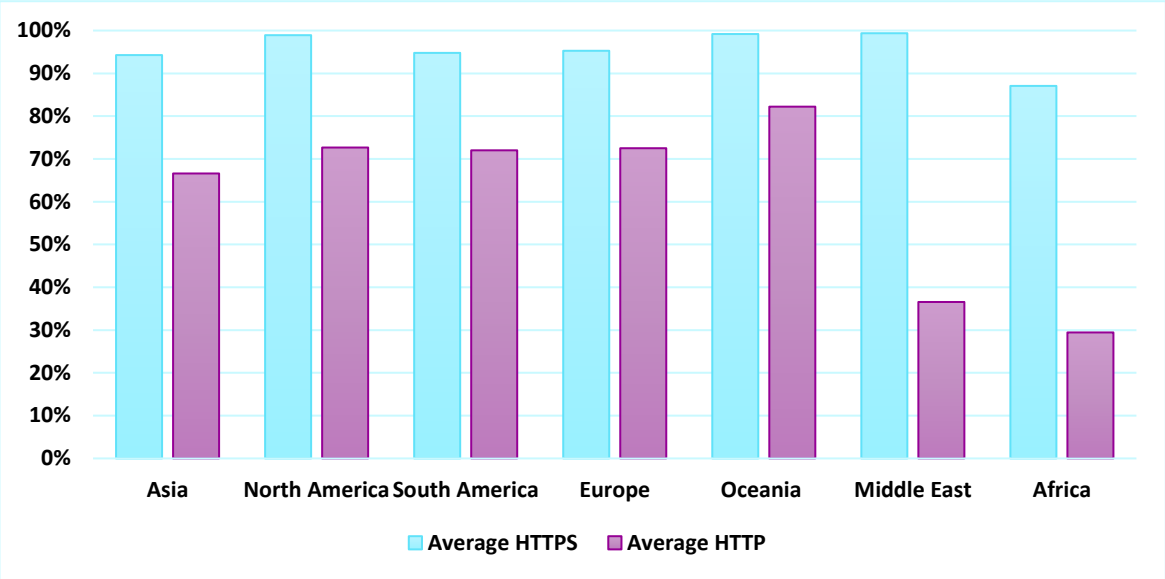

Figure 12. Censys – Average HTTPS vs HTTP per region

Censys detected a small percentage of **Telnet** connections. Telnet is an old protocol developed in 1969 and was substituted by SSH (Telnet is currently considered unsafe). We suggest all banks with Telnet to do an exhaustive examination of the protocols in place, as this could be a way for an attacker to harm the bank security.

4.3.2 Location of Services

For the banks, it is vital to have control over their information policies. Therefore, the location of the servers is of utmost importance, since it is where the data is physically located. This is why the location analysis of the different detected servers was included in our report.

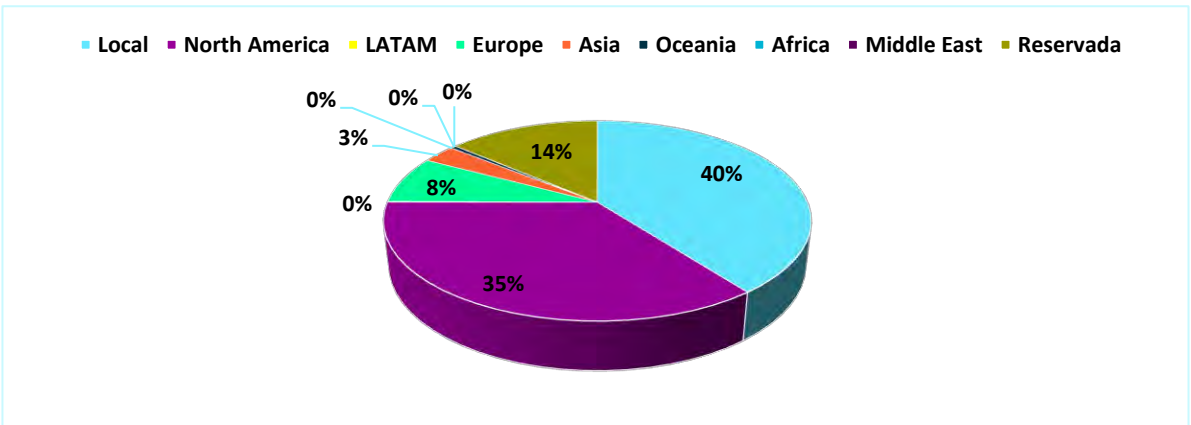

Figure 13. Censys – Services location

As can be seen above, most of the service provided is either locally hosted (40%) or in North America (35%).

Having the services located in the country where the bank is from is a good practice since it is usually easier to protect and to assure the bank follows the regulations of the country regarding data protection. Africa and Middle East are the regions where most countries keep their services locally.

It is also important to note that most of the banks use **Akamai**[2], which was included in our Censys search. Most of Akamai's services are offered from the United States and that is why we are seeing the biggest percentage on that country, followed by the Netherlands in Europe. **Using a service such as Akamai is also a good security practice.**

5. Conclusions

5.1. Mobile Applications

- We found that all banks, regardless of their location and revenue had vulnerabilities on their official applications. Considering the amount of confidential customer data they deal with, this is a serious issue.
- The analysis showed that the overall risk score was of **7.27 (High)** with banks in Asia, Africa and South America having the highest score.
- We found several vulnerabilities in the analyzed mobile applications, mainly caused by code quality flaws. The most common vulnerability was the **Potential SQL Injection**.
- We compared what permissions each banking application asked for. Despite being in the same industry and providing the same service, there was only one common permission across all applications – **Internet access**.
- Some African banks have never had any mobile app (at least we could not find them), fact aligned with Internet news about how some countries have not developed their mobile apps market.
- The average number of permissions asked by a banking app was **19**. The Middle East was the region with the lowest average number of requested permissions while Asia was the one with the highest.
- Intrusive permissions such as *CALL_PHONE*, *READ_CONTACTS*, *READ_SMS*, *WRITE_SMS*, *READ_CALENDAR* and *WRITE_SETTINGS* were present in several applications.

[2] Akamai is a content delivery network (CDN) and cloud services provider. Other companies use their services to distribute content on servers located all over the world. This means that when you download something from one of those companies, the file will be accessed from a server physically near you, resulting in a faster download speed.

5.2. Metadata on public files

- We detected **289 admin accounts** and several generic accounts with characteristics of administrators.
- The technological infrastructure of most of the banks may still be using operating systems currently not supported by their manufacturers. We cannot confirm this because the files may have been published many years ago **whilst the technology could have been updated**.
- **Over 3000 software-related metadata** were found, most of them being older versions no longer supported by their developers. An attacker could try to use exploits for these software to access the organization network.
- The analysis of public files has also given us **physical locations and names of several servers and printers**. This information should not be public due to the possible implications it may cause if a malicious actor wanted to cause harm.
- For the preparation of this report, we analyzed other aspects apart from those mentioned in the introduction:
    - Operating systems and their users.
    - IP address locations.
    - E-mail accounts associated with the metadata of the public documents downloaded.

It is possible to improve these banks' security avoiding data exposition through the **implementation of manual or automated procedures and controls**, on the technological infrastructure and on their users.

5.3. Hosts

- **Over 96%** of the identified hosts used **HTTPS**.
- There is still a great amount of **HTTP** services, which is **considered a non-secure protocol**.
- About **50%** of the banks considered **use Akamai**. This implies the traffic is going mainly through North American servers.
- **Banks not using Akamai tend to host their services locally**. The only exception is Asia, where banks that do not work with Akamai have also their servers in the USA.
- **None** of the analyzed banks from Africa uses Akamai. This is one of the regions with more local hosts.
- One of the hosts related to a bank from Africa is **Heartbleed vulnerable**. **Heartbleed** is a security bug in the OpenSSL cryptography library, an implementation of the TLS (Transport Layer Security) protocol.
- The most popular service when there is no Akamai involved is **FTP**, followed by **SMTP** and different kinds of databases.
- Most of the services are hosted in **North America**. **Europe** seems to be the second best option but with a huge gap compared to NA.
- **Africa** is the region where most of their services are locally hosted **(92%)** followed by the **Middle East (70%)**.

About the Telco Security Alliance

The alliance, integrated by Telefónica, Etisalat, Softbank and Singtel, is one of the world's biggest cyber security providers, with more than 1.2 billion customers in over 60 countries across Asia Pacific, Europe, the Middle East and the Americas. Through their combined resources and capabilities, the group can protect enterprises against the rising cyber security risks as the information security environment becomes increasingly complex.

Through the alliance, members can achieve operational synergies and economies of scale that will eventually help lower costs for their customers. The group's members operate 22 world-class Security Operation Centres (SOCs) and employ more than 6,000 cyber security experts. To expand their global footprint, the alliance is open to bringing in new members over time.

Under the agreement, the group will share network intelligence on cyber threats and leverage their joint global reach, assets and cyber security capabilities to serve customers worldwide. Leveraging each member's respective geographic footprint and expertise, the alliance is able to support each other's customers anywhere and anytime, allowing them to respond rapidly to any cyber security threats.

To enhance their cyber security portfolio, the members will also look into the possibility of developing new technologies such as predictive analytics using machine learning and advanced cyber security for the Internet of Things. The alliance will also consider developing a joint roadmap for the evolution of their security portfolios and explore joint investments in security products and services, SOCs, platforms, start-ups and R&D.