About the editors

TDS Telefónica

The CyberThreat Service of Telefónica has as its primary objective the generation of intelligence, fitted to our customers’ needs in order to counteract those threats related to the digital environment. Therefore, what differentiates Telefónica from other traditional security services is our capability to integrate, evaluate and transform raw information and data into conclusions and future scenes. The three Service bases are the following:

- Detection
- Analysis and interpretation
- Prospective and anticipation

Kaspersky Security Network

This report uses data from KSN (Kaspersky Security Network). KSN is a distributed network designed for the real time processing of threats against Kaspersky users. The objective of KSN is to be sure that all users have information on threats as soon as possible. New threats are added to the data base minutes after their detection, even if they were previously unknown. KSN also retrieves statistical non-personal information about any malicious code installed on our customers’ devices. Kaspersky Lab customers are free to join KSN, or not, as they wish.
Main findings

This report analyzes the current trends related to financial phishing and banking malware, including attacks on mobile devices, POS (Point of Sales) systems and ATMs. It is mainly based on statistics and data from KSN (Kaspersky Security Network) although reliable information from other sources may also be referenced. The timeframe for this analysis contains data obtained during the period from October 1st, 2015 to January 1st, 2016. The main findings are as follows:

Phishing

A group of 14 countries are on the receiving end of 88.42% of all phishing attacks. The remaining 11.58% is distributed among 167 different countries. Mexico, United States and Brazil accounts suppose almost half of the worldwide detected attacks, followed by Germany and Canada.

Mexico have shown the biggest percentage of phishing attacks of the entire year, even surpassing the percentage from Germany in Q3 which was the most attacked country at that moment.

United Kingdom and Italy are the most attacked European countries.

Phishing messages targeting the financial sector (banks, payment systems and online shops) accounted for 43.38% in this period, an increase of 13.19 % compared with the data analyzed in Q3 2015.

Banking malware

The number of infections of the Zeus Trojan and its variants keeps decreasing for the third period in a row during this year.

Although the Dyre Trojan decreases its percentage (representing the 19.21% of all the infections performed by banking Trojans in Q4) it keeps being the lead actor in the banking malware area.

The small banking families’ percentages have increased since Q3. Within this subset, one of the families with more activity during 2015 keeps being Tinba, increasing its activity especially against Spanish banks.
Mobile malware

Android keeps being the most frequently targeted platform. 99.78% of the mobile malware detected target this operating system.

Russian Federation, followed distantly by Vietnam and Ukraine have almost the 90% of infections according to our data. Germany, Poland and France are the most infected European countries.

A new Trojan named TinyV affecting Apple iOS devices have been detected during this period. Although the impact was mainly located in China, we detected some infections in Germany, Spain and France.

Two new Android banking Trojans have been discovered during this period. The Trojans are focused on stealing bank credentials for more than 50 banking apps (including Chinese, German, Australian, Spain, New Zealand, and USA).

UK and Spain are in a similar position than last Q in the ranking of countries infected by mobile malware.
# Table of contents

- **ABOUT THE EDITORS** | 2
- **MAIN FINDINGS** | 3
- **TABLE OF CONTENTS** | 5
- **INTRODUCTION** | 6
- **PHISHING** | 10
- **MALWARE** | 22
- **MOBILE BANKING THREATS** | 46
- **CONCLUSIONS** | 55
Introduction

October was designated as the National Cyber Security Awareness Month\(^1\) by US President Obama and European Cyber Security Month (ECSM)\(^2\) by The European Union Agency for Network and Information Security (ENISA) and Partners.

Unfortunately, neither of these initiatives stopped the criminals nor a bit. Criminals keep increasing efforts in malware distribution, for instance at the end of October a malvertising campaign redirected German users visiting ebay.de and T-online.de to the Angler exploit kit. The latter website was abused in a campaign installing NeverQuest, a known family Trojan that additionally installed POS malware (AbaddonPOS\(^3\)) in the infected system.

Regarding banking malware, one of the most relevant news is the take down of multiple command-and control (C&C) servers used by the Dridex banking Trojan in the US resulting in the seizure of multiple servers used by this malware. Dridex, considered the successor of Crídedx banking malware and operated from Eastern Europe is used to steal online banking details. Currently the International task force is ‘sinkholing’ the infrastructure and stopping infected computers from communicating with their command and control servers. Although these measures are necessary, it is still early to know its real effectiveness due to the unique nature of these complex criminal infrastructures which has been proven to be highly resistant.

Although this year we witnessed several takedowns of major banking Trojan’s infrastructure, new developments keeps emerging. During this period two new families have been identified: Win32.Shiful and Telax. Both implement the usual features for such malware but in the case of Telax (affecting mainly Brazilian and Spanish users) it leverages Google Cloud Servers to host its resources.

Tinba, a well-known Trojan banker that we have featured several times in our reports, focused on Spain with a specific campaign during Q4.


\(^2\) [https://cybersecuritymonth.eu](https://cybersecuritymonth.eu)

At the end of Q3 we mentioned the increase of DDoS (Distributed Denial of Service) attacks against financial institutions, especially those performed by the threat actor DD4BC, responsible for several Bitcoin extortion campaigns during this year. The attacks performed by this group continues, although several copycats have been identified using the same modus operandi. Perhaps the most prolific one is the collective named Armada Group that has been very active in this period launching several extortion campaigns mainly against banks, and against hosting and mail providers. One of the victims was Protonmail from which the attackers demanded 15 BTC (6000 €) to stop the attack. After the victim paid the ransom the attacker launched an additional attack. In addition to mail and hosting providers (Neobox, Runbox, Zoho, Hushmail) Armada is launching several attacks against financial institutions. As a recommendation, it is more suitable to invest money in legitimate services such as DDoS mitigation than paying to the criminals. Several victims have successfully mitigated these attacks using these services.

Throughout the year we witnessed the increase of new developments in the POS malware arena. In this Q new families have been discovered such as ModPos and Kuhook, the latter related to the ModPos family and both of with a remarkable impact in the retailer sector. Apparently this POS family is suspected to be owned and operated by a closed group, meaning that it is not currently distributed in online underground forums. The level of customization in some of the identified samples could be an indicator that the group behind chooses its targets carefully not pretending to perform massive infections in order to stay under the radar.

The detection of critical vulnerabilities for Android was one of the more remarkable events of the year. Stagefright vulnerabilities allow an attacker to remotely execute arbitrary code on a device by sending a specially crafted MMS to the victim’s number. Statefright 2.0 was disclosed in October, this time using MP3 and MP4 files that execute their payload when played using the Android Media server. Android 1.5 through 5.1 is vulnerable to this new attack and it is estimated 1 Billion devices are affected.

4 https://protonmaildotcom.wordpress.com/2015/11/05/protonmail-statement-about-the-ddos-attack/
At the very end of September Europol published the 2015 Internet Organized Crime Threat Assessment (IOCTA)\(^5\) which reflects the current cybercrime threat landscape in this region. We recommend reading it to gain insights about these organizations’ efforts to combat cybercrime.

Finally, December was a busy month for Europol which conducted two remarkable operations against cybercrime:

The first one was a two week long coordinated action against the use of remote access Trojans (RATs). Operation Falling sTAR\(^6\) resulted in multiple house searches and the arrest of 12 individuals in France, Norway and Romania.

The second, On 3 December 2015, joining forces with Joint Cybercrime Action Taskforce (J-CAT), alongside INTERPOL, the Department of Homeland Security, the FBI, the National Cyber Investigative Joint Taskforce - IC4 and law enforcement officials from across the world, including operatives from Belgium, France, Lithuania, Spain and the Netherlands partnered with Microsoft and other members of the private sector to disrupt Win32.Dorkbot, active since 2011. Besides being a simple password stealer, the infection of Dorkbot usually carried out the installation of additional malware as Denial of Service and SPAM bots, increasing its impact.

**Methodology**

This report focuses on the timeframe from October 1\(^{st}\), 2015 to January 1\(^{st}\) 2016, although several references to past analysis are included. It includes data on phishing attacks, financial malware and mobile threats, including their geographical distribution and number of attacks.

To generate statistics about banking malware we have used a selection of families traditionally seen in online fraud, including some verdicts used for stealing credentials. In the case of malware targeting points of sale devices, in addition to identifying the main known families we’ve included specific samples that do not fit in any known POS malware classification.

---


6 https://www.europol.europa.eu/content/joint-international-operation-targets-users-remote-access-trojans-across-europe
Please note that our stats are based on our verdicts, which sometimes depends on the AV engine that first detects that particular malware. For instance, if the Heuristic engine detects a piece of malicious code with a generic verdict, the details of the family it belongs to may not be reflected in the statistics.
Phishing

During this year we reviewed some of the most used baits by this scheme, using seasonal reclaims in the campaigns to increase its impact and persuasiveness. During the summer it was travel themes, fake notifications from booking services and airlines and hotels. In this period the most remarkable date is the Christmas season and so are most of the baits used in campaigns.

Reclaims using delivery services seems one of the preferred choices of the season. We observed a huge number of campaigns sending Emails pretending to be from these type of services. The image below is an example.

![Image of SPAM pretending to come from a delivery service.](image)

Figure 1. SPAM pretending to come from a delivery service.

During this year, phishing campaigns have maintained a steady number of affected users when compared with 2014. The phishing distribution graph (Figure 2) keeps showing the characteristic fluctuations for the campaigns, although they were quite intense during December.

The following graph shows the number of users receiving phishing attacks detected during the last period of 2015:
The following map shows the countries with the greatest total number of victims attacked by phishing campaigns:

According to this geographical distribution, the countries with a higher number of victims attacked by phishing are Mexico, United States, Brazil, Germany and Canada. Following this list are the United Kingdom and Italy.
The big surprise for this period’s analysis came from Mexico, which showed the biggest percentage of phishing attacks of the entire year, even surpassing the percentage from Germany in Q3 who was the most attacked country until Q3 2015.

The graph in Figure 4 shows the group of countries that are on the receiving end of 88.42% of all phishing attacks. The remaining 11.58% is distributed among 167 different countries.

Germany which traditionally has been in the first position of this ranking during most of 2015, now drops to the fourth place with 7.28% of all detected phishing. Something similar can be observed with the attacks detected against Italian users, which have decreased significantly when comparing the data with past’s periods (from receiving 8.42% of attacks during Q3 2015 to 6.12 % in this period).

Mexico and the United States are still in the top 3 of top targeted countries in Q4, as it happened during Q3 2015. The graph below shows the global distribution of phishing attacks per country:

![Figure 4. Percentage of total phishing attacks - distribution by country | Q4 2015](image)

The graph in Figure 5 compares the percentage of attacks by countries with previous periods. There are several changes worth noticing. Mexico which we already detected showing a remarkable increase during Q3 2015 (it raised 6 positions in the global ranking) reaches the top position of the entire year with a 27.16 % of all the phishing
attacks during this period. We noticed a similar peak in Q3 2015 in Germany which accounted for 26.82% of attacks.

Attacks against Brazil have increased significantly (from 1.18% to 9% in this Q).

Finally, we’ve observed an increasing trend in Japan’s percentages during this Q, especially when compared with the rest of the year.

Germany, UK and Italy are the European countries with higher percentages, with Germany in the first place in the European ranking. These three together represent more than 20% of the World’s total phishing activity.

Spain moves to the 14th position globally (it was 15th in Q3), positioning itself to a better place in the ranking for the third time this year. In the last few months of 2014 Spain was the 12th country among the most affected ones worldwide.

Complementing the geographic distribution of attacks, the figures below show the percentage of infected users in each country. This perspective shows a different but consistent picture.
Figure 6 shows the evolution of the percentage of users affected per country:

New Zealand was the country that suffered more phishing attacks per user over the course of Q3 2015 and now has been displaced by Mexico which shows an alarming increase of users affected by phishing.
The table below shows the same information for the European Union countries (plus UK). Since the beginning of 2014 we have seen several changes in this classification. UK, Italy and Austria are the European Union countries with the highest percentage of users affected by phishing, followed by Luxembourg and Portugal.

![Figure 7. Percentage of users affected by phishing - EU countries | (2014 - 2015)](image)

The percentages of users affected by phishing in Europe have decreased when compared to previous periods. In addition, the incidence of the attacks is being distributed among more countries.

The number of attacks against Spain has increased, although we observe similar levels than the ones observed during most of 2014.

Phishing messages targeting the financial sector (banks, payment systems and online shops) accounted for 43.38% in this period, an increase of 13.19% compared with the data analyzed in Q3 2015.
Within the financial area, the banking sector continues to be by far the most common target, continuing the same trend seen during the whole 2014 and 2015.
For most of 2014 there was a high percentage of phishing attacks targeting a relatively small group of banks. This shows a very clear long tail distribution, with few targeted banks representing most of the attacks and the rest spread among a long group of organizations. This trend is consistent with the one observed during this period, on which the long tail represented 37.03% of the attacks. During this period the long tail accounts for 36.58% of all the attacks.

The following graph shows the target distribution for the main targeted entities.

The chart below shows the countries of origin of the most frequently targeted banks. It is worth noting some relevant indicators observed in this period. First the increase in attacks targeting Brazilian banks detected during 2015 continues, although in Q4 they have decreased for most of them, it seem that there is a specific bank in that region that is concentrating most of the attacks. Secondly, there has been a huge increase in detected attacks against a specific Indian bank. This entity received a 4.10% of all the attacks but in this period the percentage is the 9.50%.
Brazil (36%), the United States (17%) and India (15%) are the top three countries of origin for the most frequently targeted banking organizations:

Figure 11. Phishing target bank distribution by country of origin | Q4 2015

Phishing attacks against UK banks have increased during this period, from 4.63% in Q3 to 9% in Q4. Spain is in a similar position than in 2014, although since Q3 their banks are being the target of more attacks (from 3.03% during Q3 215 to 6% now).
The following table provides the data distributed over the last 24 months:

![Figure 12. Phishing target bank distribution by country of origin of the targeted entities - (2014 - 2015)](image-url)
In the online payment sector there is still little more to choose other than the three top targets. These didn’t change over the past two years. PayPal, Visa, American Express and MasterCard continue to be by far the most targeted entities, just as in 2013 and 2014.

Regarding e-commerce targeted by phishing attacks, during the first months of 2015 one of the most remarkable trends was the big increase of attacks against Steam (online game distributor and social networking platform developed by Valve Corporation) users. Although the numbers for Q3 showed a decrease in such attacks, during this last period it has suffered an astonishing increase, from 17.59% in the past period to 41.79% in Q4 2015. A logical explanation for this increase could be the Christmas season and the raise of activity in the online gaming world, from the increase in purchases to the growth in the number of players interacting with Steam.
The following chart shows the big picture about phishing attacks against e-commerce sites:

Figure 14. Phishing target distribution - E-Commerce | Q4 2015
Malware

This section analyzes the impact of banking malware from a global perspective, with a special focus on Spain and the UK.

The first chart shows the distribution of banking malware among global users during Q4 2015:

![Banking malware global distribution by families | Q4 2015](image)

Infections by Zeus Trojan and variants keep decreasing for the third time during this year (from 14.94% in Q2 to 14.26% in Q3 and now 12.6%).

One of the most remarkable points in this period is the decrease of the banking Trojan Dyre. This Trojan now represents the 19.21% of all the infections performed by banking trojans during this period (during Q3 2015 this percentage was 25.14%).

The small banking families’ impact that decreased slightly during Q3 has increased since then. Within this subset, one of the families with more activity during 2015 keeps being Tinba, and although during Q3 its activity decreased, now shows the higher percentage of infections of this year. Tinba now accounts for 2.01% of all the small families’ infections, a difference of +0.87% when compared with Q3 2015. In
addition, infections performed by Chepro (a banking Trojan originally from Brazil) have increased notably during this period.

These bankers are distributed as follows:

![Chart showing banking malware distribution]

**Figure 16. Banking malware distribution - Small banking families | Q4 2015**

The graphic below shows how these banking families evolved from 2014 until the end of 2015:
From the previous charts:

“Other” refers to all malware related to the distribution of banking malware, such as known downloaders usually tied to banking malware families. However they are not in themselves banking Trojans.

“Other bankers” includes different banking Trojans that do not belong to any well-defined banking family. This category can also contain malware detected by our heuristic engine and analyzed based on other patterns (hashes, behavior, techniques implemented, etc.).

Finally, “Small bankers” are banking families that are well known, but don’t have high levels of distribution compared with the most popular current malware.
We can see more detail about the distribution of banking Trojans worldwide during the analyzed period.

### Table I: Global distribution of banking threats | Q4 2015

<table>
<thead>
<tr>
<th>Family</th>
<th>% of infections against the total (banking Trojans)</th>
<th>Q4 2015</th>
<th>Difference compared with Q3 2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zeus family</td>
<td>12,60</td>
<td>-1,66</td>
<td></td>
</tr>
<tr>
<td>Tepfer</td>
<td>8,01</td>
<td>0,70</td>
<td></td>
</tr>
<tr>
<td>Other bankers</td>
<td>39,58</td>
<td>4,69</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>1,43</td>
<td>-1,41</td>
<td></td>
</tr>
<tr>
<td>Keylogger</td>
<td>2,31</td>
<td>-0,41</td>
<td></td>
</tr>
<tr>
<td>Bitcoin Miner</td>
<td>4,10</td>
<td>1,52</td>
<td></td>
</tr>
<tr>
<td>Dyre</td>
<td>19,21</td>
<td>-5,93</td>
<td></td>
</tr>
<tr>
<td>Qhost</td>
<td>7,65</td>
<td>0,91</td>
<td></td>
</tr>
<tr>
<td>Small banking families</td>
<td>5,11</td>
<td>1,59</td>
<td></td>
</tr>
</tbody>
</table>

### Table II: Global distribution of small banking families in Q4 2015

<table>
<thead>
<tr>
<th>Family</th>
<th>% of infections against the total (banking Trojans)</th>
<th>Q4 2015</th>
<th>Difference compared with Q3 2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small banking families</td>
<td>5,11</td>
<td>1,59</td>
<td></td>
</tr>
<tr>
<td>Hlux</td>
<td>0,37</td>
<td>-0,06</td>
<td></td>
</tr>
<tr>
<td>Carberp</td>
<td>0,25</td>
<td>0,09</td>
<td></td>
</tr>
<tr>
<td>Sinowal</td>
<td>0,23</td>
<td>-0,01</td>
<td></td>
</tr>
<tr>
<td>Shiz</td>
<td>0,13</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>ChePro</td>
<td>1,44</td>
<td>1,44</td>
<td></td>
</tr>
<tr>
<td>NeverQuest</td>
<td>0,02</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Neurevt</td>
<td>0,39</td>
<td>0,03</td>
<td></td>
</tr>
<tr>
<td>Tinba</td>
<td>2,01</td>
<td>0,87</td>
<td></td>
</tr>
<tr>
<td>Emotet</td>
<td>0,13</td>
<td>-0,04</td>
<td></td>
</tr>
<tr>
<td>Metel</td>
<td>0,14</td>
<td>-0,37</td>
<td></td>
</tr>
</tbody>
</table>

The rest of this section focuses on banking malware in Spain and the UK.

The first chart compares these countries’ positions in a world ranking for the number of banking malware infected users (first in the ranking is the country with most percentage of infected users) from 2014 until the end of 2015. It must be noted that the malware families (verdicts) used in this ranking varies over time:
In comparison to last year, Spain has worsened its situation continuing the trend observed since then. The UK has been more stable in terms of ranking positioning during 2015 improving its position quarter after quarter.

The countries with most banking malware detections during this period were:

| Table III: The countries most affected by banking malware in Q4 2015 (global, % of users infected) |
|---------------------------------------------------|---------------------------------------------------|
| Country                                           | Percent of users                                 |
| Russian Federation                                | 32.12 %                                           |
| Brazil                                            | 26.96 %                                           |
| Germany                                          | 7.05 %                                            |
| India                                            | 5.09 %                                            |
| Republic of Iran                                  | 4.66%                                             |
| Vietnam                                          | 4.36%                                             |
| Austria                                          | 3.51 %                                            |
| Mexico                                           | 3.33%                                             |
| United States                                    | 3.02%                                             |
| Spain                                            | 2.38%                                             |
The first three countries in Table III represent the 66.13% of global infections; the rest is divided between 192 countries.

The following graph shows the top ten countries most affected by banking malware:

![Graph showing top ten countries affected by banking malware]

Figure 19. Countries most affected | Q4 2015 (GLOBAL, % of attacks)

The most affected European Union (plus UK) countries during this period were:

<table>
<thead>
<tr>
<th>Country</th>
<th>% of users infected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Germany</td>
<td>4.22 %</td>
</tr>
<tr>
<td>Austria</td>
<td>2.35 %</td>
</tr>
<tr>
<td>Spain</td>
<td>1.28 %</td>
</tr>
<tr>
<td>France</td>
<td>1.13%</td>
</tr>
<tr>
<td>Poland</td>
<td>0.94%</td>
</tr>
<tr>
<td>Italy</td>
<td>2.06%</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>1.43%</td>
</tr>
<tr>
<td>Portugal</td>
<td>1.19%</td>
</tr>
<tr>
<td>Greece</td>
<td>0.09%</td>
</tr>
<tr>
<td>Belgium</td>
<td>0.09%</td>
</tr>
</tbody>
</table>
The following graph shows the distribution:

![Graph showing countries most affected by banking malware | Q4 2015 (EU, % of users infected)](image)

**Figure 20. Countries most affected by banking malware | Q4 2015 (EU, % of users infected)**

During this period banking malware in Germany, Italy and Spain had a significant growth compared with the same period of the last year. On the other hand, although Germany shows less percentage than the observed in Q3 it keeps maintaining the first position in the ranking.
The following chart analyzes the distribution of banking threats in Spain:

![Pie chart showing distribution of banking malware by family.]

**Figure 21. Distribution of banking malware by family - Spain | Q4 2015.**

There are several points worth mentioning from figure 22:

First is the slightly decrease of Dyre for the first time in 2015. Zeus follows the decreasing trend observed since the beginning of this year, and their percentage drops from 18.86% to 12.44% in this period.

The “Small families” group has increased notably during this period in Spain. Clearly this is related to several campaigns performed by Tinba against online banking users in Spain, especially during the last quarter of year. The percentages of Tinba have raised from 1.45% in Q3 to 6%.
The following table compares the last two analyzed periods for Spain:

### Table V: Global distribution of banking threats in Spain | Q4 2015

<table>
<thead>
<tr>
<th>Families</th>
<th>% of infections against the total (banking Trojans)</th>
<th>Q4 2015</th>
<th>Difference compared with Q3 2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zeus family</td>
<td>12.44</td>
<td></td>
<td>-6.42</td>
</tr>
<tr>
<td>Tepfer</td>
<td>7.09</td>
<td></td>
<td>7.09</td>
</tr>
<tr>
<td>Other bankers</td>
<td>19.41</td>
<td></td>
<td>0.59</td>
</tr>
<tr>
<td>Other</td>
<td>0.98</td>
<td></td>
<td>-0.26</td>
</tr>
<tr>
<td>Keylogger</td>
<td>0.45</td>
<td></td>
<td>0.08</td>
</tr>
<tr>
<td>Bitcoin Miner</td>
<td>0.24</td>
<td></td>
<td>-0.08</td>
</tr>
<tr>
<td>Dyre</td>
<td>48.42</td>
<td></td>
<td>-5.82</td>
</tr>
<tr>
<td>Qhost</td>
<td>3.76</td>
<td></td>
<td>-0.08</td>
</tr>
<tr>
<td>Small banking families</td>
<td>14.3</td>
<td></td>
<td>11.99</td>
</tr>
</tbody>
</table>

The following table shows the variations in the percentage of infections for small banking family:

### Table VI: Global distribution of small banking families in Spain | Q4 2015

<table>
<thead>
<tr>
<th>Small banking families</th>
<th>% of infections against the total (banking Trojans)</th>
<th>Q4 2015</th>
<th>Difference compared with Q3 2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small banking families</td>
<td>14.3</td>
<td></td>
<td>11.99</td>
</tr>
<tr>
<td>Hlux</td>
<td>0.17</td>
<td></td>
<td>0.07</td>
</tr>
<tr>
<td>Carberp</td>
<td>0.09</td>
<td></td>
<td>0.07</td>
</tr>
<tr>
<td>Sinowal</td>
<td>0.52</td>
<td></td>
<td>0.07</td>
</tr>
<tr>
<td>Shiz</td>
<td>0.04</td>
<td></td>
<td>0.01</td>
</tr>
<tr>
<td>ChePro</td>
<td>0.13</td>
<td></td>
<td>0.13</td>
</tr>
<tr>
<td>NeverQuest</td>
<td>0.06</td>
<td></td>
<td>0.01</td>
</tr>
<tr>
<td>Neurevt</td>
<td>0.17</td>
<td></td>
<td>-0.04</td>
</tr>
<tr>
<td>Tinba</td>
<td>6</td>
<td></td>
<td>4.55</td>
</tr>
<tr>
<td>Metel</td>
<td>-</td>
<td></td>
<td>0.13</td>
</tr>
</tbody>
</table>
The following table shows the changes in the distribution of Trojan banking families in Spain over 2014 and 2015:

![Figure 22. Distribution of banking malware by family - Spain | 2014 - 2015.](image)

In the UK the distribution of banking threats is as follows:

![Figure 23. Distribution of banking malware by family - UK - | Q4 2015](image)
For third time in 2015 Dyre have had more impact in the UK (50.78%) during this period than in Spain (48.42%) and both countries exceeds by far the global percentages affectation of 19.21%. Nevertheless we observed a drop in the Dyre percentages during this period, dropping from 60.58% in Q3 to 50.78% in Q4.

The distribution for small banking families is as follows:

![Diagram of distribution for small banking families UK | Q4 2015](image)

The Small banking family’s percentages present no surprises when comparing the data with past periods.
The following table shows the difference in the percentage of infections for banking Trojan families:

### Table VII: Global distribution of banking threats in UK | Q4 2015

<table>
<thead>
<tr>
<th>Families</th>
<th>% of infections against the total (banking Trojans)</th>
<th>Q3 2015</th>
<th>Difference compared with Q2 2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zeus family</td>
<td>10.60</td>
<td>-1.01</td>
<td></td>
</tr>
<tr>
<td>Tepfer</td>
<td>0.03</td>
<td>0.03</td>
<td></td>
</tr>
<tr>
<td>Other bankers</td>
<td>20.27</td>
<td>0.20</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>14.49</td>
<td>10.67</td>
<td></td>
</tr>
<tr>
<td>Keylogger</td>
<td>0.89</td>
<td>0.37</td>
<td></td>
</tr>
<tr>
<td>Bitcoin Miner</td>
<td>0.89</td>
<td>0.29</td>
<td></td>
</tr>
<tr>
<td>Dyre</td>
<td>50.78</td>
<td>-10.07</td>
<td></td>
</tr>
<tr>
<td>Qhost</td>
<td>0.46</td>
<td>-0.30</td>
<td></td>
</tr>
<tr>
<td>Small banking families</td>
<td>1.59</td>
<td>-0.18</td>
<td></td>
</tr>
</tbody>
</table>

The next figure shows the differences in the percentage of infections for small banking families:

### Table VIII: Global distribution of small banking families in UK | Q4 2015

<table>
<thead>
<tr>
<th>Small banking families</th>
<th>% of infections against the total (banking Trojans)</th>
<th>Q4 2015</th>
<th>Difference compared with Q3 2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small banking families</td>
<td>1.59</td>
<td>-0.18</td>
<td></td>
</tr>
<tr>
<td>Hlux</td>
<td>0.19</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Sinowal</td>
<td>0.07</td>
<td>-0.16</td>
<td></td>
</tr>
<tr>
<td>Shiz</td>
<td>0.04</td>
<td>0.01</td>
<td></td>
</tr>
<tr>
<td>NeverQuest</td>
<td>0.05</td>
<td>0.03</td>
<td></td>
</tr>
<tr>
<td>Neurevt</td>
<td>0.44</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Tinba</td>
<td>0.57</td>
<td>-0.06</td>
<td></td>
</tr>
<tr>
<td>Emotet</td>
<td>0.13</td>
<td>0.13</td>
<td></td>
</tr>
<tr>
<td>Marcher</td>
<td>0.05</td>
<td>0.05</td>
<td></td>
</tr>
</tbody>
</table>

The following table shows the evolution for the share of infections for the main banking malware families in the UK:
Figure 25. Distribution of banking malware by family UK | 2014 - 2015
Remarkable threats

This section analyzes some of the banking families that have made an impact or have evolved significantly during this year.

Dyre

Dyre has been without a doubt the lead actor in the banking malware area during 2015. In addition to the impact observed in the statistics, it is known that the development of the trojan capabilities as well as the distribution component is really active, making this trojan one of the most dangerous threats for online banking users.

Kaspersky Lab products detect Dyre malware mostly with heuristics and proactive technologies with the verdict Trojan-Banker.Win32.Dyre and its downloader module as Trojan-Downloader.Win32.Upatre.

During this period the percentages for Trojan-Downloader.Win32.Upatre have decreased notably, as the diversification of Dyre’s distribution channels decreased the importance of this dropper.

The following graph shows the number of infections by Trojan-Downloader.Win32.Upatre:

![Figure 26. Upatre infections | Q4 2015](image-url)
The following map shows the geographic distribution of infections:

Figure 27. Geographical distribution. Upatre | Q4 2015

Germany is by far the most affected country globally. Within the European Union, Germany, Spain and Austria are the first ones in the ranking.

Figure 28. Geographical distribution. Upatre | Q4 2015
Tiny Banker (Tinba)

Within the "Small banking families" subset, Tinba has been the leading family for most of 2015. The statistics observed throughout the year shows the typical fluctuation that coincides with the Modus Operandi of closed groups launching specific and controlled campaigns. The new Tinba version keeps focusing strongly in attacking European Banks. We’ve observed three spikes, the first at the end of June 2015, the second at the beginning of September and finally at the end of December.

The following graph shows the distribution of infections for Q4 2015:

![Figure 29. Tinba infections | Q4 2015](image)

Germany is the country with higher percentages of Tinba detections, followed distantly by United Arab Emirates and India. Within Europe, Germany, Austria and Spain are the top three countries in the ranking.
Figure 30. Tinba percentage of infections per country | World | Q4 2015
Banking Trojan configuration files

This section analyzes the configuration files used by banking Trojans. These configuration files contain a list of targets and details on how the malware should interact with them. Usually they redirect their victims to other phishing or malicious websites when browsing one of the targets in the list, or inject code into the browser to ask for additional login data. More advanced code injections try to carry out Automatic Malicious Transactions (AMTs) without the victim’s knowledge.

The analyzed data includes configurations collected from the main Trojan families from October 1, 2015 until January 1, 2016. There are some points worth mentioning about Trojan configuration analysis:

- A single configuration file may be reused multiple times.
- Every configuration file includes details of dozens of targets and what the malware should do with each of them.
- These configuration files may change depending on the location of the victim.

First of all we can see the countries where the targeted entities are based, in this case drawn from references in configuration files:

![Figure 31. Number of total entries in configurations files by country of origin](image)

We should keep in mind that the same reference can appear several times, depending on how popular the target is among attackers.
In the stats for this period shows Germany appearing less times in configuration files than the previous periods, still it is in the top five targeted countries. Something similar happens with Canada which in Q3 was in 7th position and now it’s in the 14th place.

The following graph shows the target distribution by individual entities. Obviously bigger entities offering more services will have a greater presence in configuration files. In this chart different identical entries in configuration files are counted only once. Entities have been anonymized, only referencing their countries of origin:

![Figure 32. Most targeted entities by country of origin | Q4 2015](image)

The main characteristics of these configuration files are:

- **Targeted entity grouping:** A prevalent feature that means many of the targeted entities always appear together in configuration files.
- **Re-utilization:** Based on the grouping characteristic described above, cybercriminals tend to keep all their targets in the same configuration files and re-use them repeatedly.
- **Target consistency:** There are very few changes among the attacked entities in these configuration files. Even when targets are no longer operative there is no real benefit in removing targets from them, other than to make the configuration file a bit smaller. This may suggest that many of the groups behind these Trojans are running on auto-pilot and pay little attention to
maximizing returns from their botnets. Although we’ve seen a constant low ratio of dead links during 2015, there is still a very large number of them.

The following graph shows the total number of entries per country of origin of the affected entity found in configuration files. Please note that a single entity might be referenced multiple times depending how popular it is among Trojan banker’s configuration files:

Figure 33. Number of entries in configuration files distributed by targeted entity country | Q4 2015
Point of Sale Malware

During this year several new families have appeared: LogPOS, Punkey, FighterPOS, BernhardPOS, GamaPOS, ModPOS and so on until the approximately number of 26 known malware families included in this category (our heuristic engine identifies several samples with similar functionality that do not belong to any given family).

Due to the nature of this infection every single detection should be interpreted as an infected “device” not a “victim”. The impact, thereafter, is higher because these devices usually store and transmit a large amount of payment card information, affecting many victims. Statistics for older POS malware families such vSkimmer, FrameworkPOS, Project Hook, Alina, Dexter and Jackpots continue to show a residual impact during this period, the same trend observed over the last months.

The image below shows detections for a generic verdict that contains some of the known families.

Figure 34. Number of user affected. Generic POS verdict (Trojan-Spy.Win32.POS) | Q4 2015
The following image shows the geographical distribution of victims:

Figure 35. Geographical distribution. Generic POS verdict (Trojan-Spy.Win32.POS) | Q4 2015

Brazil, United States and China are the top three countries in the global ranking. UK Austria and France are the only European countries that appear within the top 10 positions. The Russian Federation who was on the second position during Q3 now has dropped 3 positions to the 5th position in the ranking.

Figure 36. Geographical distribution. Generic POS verdict percentages (Trojan-Spy.Win32.POS) | Q4 2015
One of the POS malware families with bigger impact throughout the year has been Backoff. During most of the 2015 we observed several pikes in the statistics, highlighting the one in July and the one observed in this period which doubles the percentage of infections detected in Q3.

![Backoff victim infections | Q4 2015](image)

The following image shows the distribution of infected users based on KSN statistics:

![Backoff Geographic distribution | Q4 2015](image)

Turkey has been by far the most affected country during this period with 16.43% of Backoff infections, a remarkable increase in respect of Q3 2015 (4.75%). The Russian
Federation which not appeared in the top 10 positions during the past period, now is in second position with a percentage of 8.45% of all detected infections. United Arab Emirates improves its position in the ranking dropping to the 4th place from the second one in Q3.

The following table shows the percentages for Q4 2015:

![Figure 39. Backoff victims per country | Q4 2015](image)
Mobile banking threats

Malware

Continuing the trend observed during the last few years Android has been the most affected platform in this period too. The platform is targeted by 99.78% of all samples detected on any mobile platform. At the end of 2014 this figure was 99.41%.

Some headline figures from the detections in the analysis period:

- We detected 163,490 malicious installation packages.
- We found 143,300 new malicious applications for mobile devices.
- There are 25,266 mobile banking samples in our database.

The number of new unique samples for mobile devices continues to increase from the beginning of the year, with 18,659 unique samples on January 1st 2015, and 25,266 in December 31st, 2015.
As more than 99% of mobile banking malware exclusively targets Android devices, and in order to avoid unnecessary noise and old verdicts, we decided to remove several verdicts affecting other mobile platforms.

The following map shows the distribution of infected users by mobile banking Trojans and related verdicts:

![Figure 41. Mobile banking trojans geographic distribution](image)

Russian Federation alone takes the 86.50% of infected users, followed distantly by the rest of countries. Germany, Italy, France, Poland and Austria are the most infected European countries.

If we take a look at the percentage of infected users within a country, the picture is slightly different but without any relevant surprises other than the increase of infections in Italy and France. The following chart shows the percentage of mobile devices infected by country (without Russia) for Q4 2015:
Spain and UK ranked 20th and 19th respectively on the global listing. The lower the ranking score, the higher the rate of infection.

Table IX: Mobile banking country positions for the UK and Spain | Global 2015

<table>
<thead>
<tr>
<th></th>
<th>Global position Q1 2014</th>
<th>Global position Q2 2014</th>
<th>Global position Q3 2014</th>
<th>Global position Q4 2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>UK</td>
<td>39</td>
<td>76</td>
<td>63</td>
<td>59</td>
</tr>
<tr>
<td>Spain</td>
<td>47</td>
<td>55</td>
<td>68</td>
<td>72</td>
</tr>
</tbody>
</table>

Both the UK and Spain decreased significantly their positions during the beginning of this year when compared with 2014, during this period Spain reaches its second best position in 2015, the same as UK.

Table X: Mobile banking country position for the UK and Spain | EU - 2015

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>UK</td>
<td>9</td>
<td>10</td>
<td>7</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>Spain</td>
<td>17</td>
<td>13</td>
<td>13</td>
<td>17</td>
<td>0</td>
</tr>
</tbody>
</table>
The table for European countries reflects the same distribution. Although traditionally Germany has occupied the first place in this ranking, during this period its percentage has increased notably.

Most European Union countries had above-average infection rates during this period.

---

**Figure 43. Banking mobile Trojan distribution by country | EU 2015 (% infected users by country)**
Remarkable threats

Faketoken.AndroidOS is a mobile threat used to redirect Transaction Authentication Numbers (mTAN) to a second device without the victim’s knowledge and it’s been one of the leading actors in the mobile malware show this year.

During 2015 we have observed several fluctuations in the statistics which maintained a decreasing trend, but all in all the number of global infections keeps being really high. During this period the percentage of Faketoken infections raised, especially at the end of the year. Germany, France, the Netherlands and Poland are the most affected European countries as they were during Q3.

The following graph shows the number of infections during Q4 2015:

![Figure 44. Faketoken infections | Q4 2015](image-url)
The following map shows the geographic distribution of FakeToken:

![Figure 45. FakeToken distribution | Q4 2015](image)

**Trojan-Downloader.iPhoneOS.Tiniv**

TiniV was discovered in October affecting users with jailbroken Apple iOS devices. Although the infections are mainly located in China, we detected some infections in Europe, concretely in Germany (1.15% of infections), Spain and France with 0.8% of infections.

One of the dangerous features of TiniV is the ability to install additional applications in the infected device and although we’ve not seen this malware downloading banking Trojans, we believe that it’s a matter of time that some threat actor start to monetize these infections by installing complementary malware.
Backdoor.AndroidOS.Torec.a is a variation of the popular Orbot Tor client that we discovered in February 2014. In the middle of May 2015, a unique encryption Trojan for Android was released for sale on a virus writers’ forum for $5,000. A few days later, we saw the appearance of a new mobile encryptor Trojan in the wild that we detect as Trojan-Ransom.AndroidOS.Pletor.a. Probably you are wondering what this has to do with financial malware, the truth is that we have observed the same author moving to banking malware development during this period.

The same author has released two more Android malware focused on banking credential stealing. Latest modifications of Acecard attacks mainly Australia, Russia, Germany and France, although it has capabilities to steal credentials from more than 50 banking apps all over the world (including Chinese, German, Australian, Spain, New Zealand, USA)
The following figure shows the number of detected infections in Q4:

Figure 47. Acecard distribution | Q4 2015

Figure 48. Acecard distribution | Q4 2015
Based on KSN data, Germany, Turkey and Poland are the three top European countries targeted by this malware:

![Acecard distribution](image)

**Figure 49. Acecard distribution | Q4 2015**

**Trojan-Banker.AndroidOS.Abacus**

The other newcomer is **Trojan-Banker.AndroidOS.Abacus** developed from the same author of the Acecard Trojan mentioned above. As it can be seen on the statistics, this malware spreads more aggressively:

![Abacus distribution](image)

**Figure 50. Abacus distribution | Q4 2015**

The impact of other mobile banking families (Wroba, Agent, Binka, Gidix, Perkel, etc.) is almost residual during this period.
Conclusions

The statistics analyzed during this year confirm that the Dyre Trojan is leading the banking malware area, and although their impact has decreased globally during the last Q of 2015, it represents one of the major threats to online banking users. There are several active Dyre botnets and although there were some arrests in 2015, they do not seem to affect the overall structure.

There are several interesting points worth highlighting:

- The alarming percentage observed in phishing attacks against Mexico could indicate an increase in foreign criminal efforts to operate in that region that traditionally has been exploited by well-established local groups. During 2015 we observed several campaigns using a more typical Brazilian modus operandi, even using the reclaims in Portuguese or using CPL file to infect users.

- From the high percentage of phishing attacks against Steam users during the entire year we can infer that criminals are taking advantage of the several opportunities that such platforms have, not only for its huge user base but also for its easy monetization possibilities.

- Based on the statistics analyzed during 2015 it’s clear that Zeus has lost its popularity in favor of Dyre. Besides its technical capabilities (it has all the features that criminals need to perform online fraud) Dyre surfaced at the appropriate time when other major banking Trojan families were shut down or leaked, attracting several affiliates that helped the Dyre “enterprise” to take traction until today.

- POS malware activity, specially related to the Backoff family shows a remarkable increase. Within the POS malware families and judging by our statistics Backoff has been one of the leading actors during 2015. There several active botnets deploying Backoff and its development is really active, a dangerous combination that is reflected on our numbers.

- Android devices have been the most affected mobiles by malware during two years in a row. We observed several new developments and malicious techniques to exploit these smartphones but perhaps one of the most relevant points in this specific area is the criminal’s diversification to other schemes such as Ransomware, which will be one trend worth watching in 2016.
- The proliferation of Trojans directed to Apple iOS devices keeps growing and it’s only a matter of time before we start seeing banking fraud and extortion schemes affecting these devices in bigger proportions.