


# PandaLabs Quarterly Report

## July - September 2012

# 01| Introduction


Trojans once again continued to account for most new malware samples and infections in the third quarter of the year. Despite much of this timeframe being a holiday period for many countries, the creation of new malware unfortunately did not slow down. As usual, our quarterly report takes a look at the countries with the highest and lowest infection rates worldwide. Once again China led the way, whereas Ireland entered the ranking of least infected countries for the first time ever.

There were hacking attacks on such important companies as Dropbox, Reuters, Adobe and Blizzard, with attackers gaining access to corporate and customer data. However, not everything was bad news. We learned of the arrest of the leader of the TeaMp0isoN collective, who hacked into the email account of former British Prime Minister Tony Blair, and a U.S. hacker who sold access to thousands of hijacked home computers.

Finally, our report also covers the latest cases of cyber-war in Morocco, China and the Middle East, as well as infections targeting consumer mobile devices.

# 02| Q3 at a glance

Over the last quarter we have seen numerous examples of hacking attacks. The Dropbox file-sharing service suffered a huge security breach that led to theft of usernames and passwords from thousands of users. According to reports, it was users themselves that raised the alarm after starting to receive spam at addresses used only for Dropbox.

## Cyber-crime

In South Korea, mobile carrier KT Corporation suffered a data breach which exposed personal information of over 8.7 million customers. Shortly after the hack, South Korean police announced the arrest of two programmers who were allegedly involved with the theft.

The Reuters news service suffered two successful hacker attacks on its blogging platform. The news agency was first hit at the beginning of August when a false interview with a Syrian rebel leader was published. As a result, Reuters took its blogging platform offline for a few hours. Two weeks later, a similar incident took place involving an article that falsely claimed Saudi Arabia's foreign minister Saud al-Faisal had died.


FIG.1. *DROPBOX.*


FIG.2. *REUTERS.*

Blizzard, the American video game developer and publisher of titles like World of Warcraft, Starcraft or Diablo, confirmed in August that they had suffered a security breach and urged users to change the login credentials to its online gaming service Battle.net. They confirmed that hackers were able to obtain users' email addresses and encrypted passwords.


FIG.03. *BLIZZARD.*

In September, it was revealed that Adobe had also been attacked by hackers. In this case though, the attackers were not interested in stealing customer data, but in accessing one of the company's internal servers to be able to sign their malware with a valid digital certificate from Adobe. The attack took place in July.

Nevertheless, apart from all these attacks, there has also been good news in the fight against cyber-crime:

Junaid Hussain of Birmingham, United Kingdom, the leader of the TeaMp0isoN collective, pleaded guilty to hacking into the Gmail account of former UK Prime Minister Tony Blair. A few weeks later he was sentenced to six months in prison.


FIG.04. *TEAMPOISON.*

Hacker Joshua Schichtel, of Phoenix, United States, received a 30-months prison sentence for hijacking 72,000 computers. More precisely, he was paid to install or have installed malware on those computers. In one case, a customer paid him $ 1,500 to install a Trojan on every computer on his botnet.

## Cyber-war

This quarter we have seen a number of cyber-espionage attacks aimed at journalists in different parts of the world.  For example, in Morocco, a group of independent journalists who received an award from Google for their efforts during the Arab Spring revolution, was infected with a Mac Trojan. In China, a group of foreign correspondents was targeted by two malware attacks via email a few weeks before the Congress of the Chinese Communist Party.


FIG.05. *SAUDI ARAMCO.*

This quarter we have also seen a couple of malware infections in companies operating in the energy sector in the Middle East. It is still not known if these incidents are related or are due to some type of cyber-attack, but all the evidence seems to indicate so. The Saudi Arabian Oil Company (Saudi Aramco) was hit by a malware infection that led the company to severe its connections to the Internet as a preventive measure.


FIG.06. *RASGAS.*

In addition to this, a virus infected Qatari natural gas company RasGas. However, neither RasGas nor Saudi Aramco saw their production halted due to these incidents.

## Mobile Phone Malware

Opera Mini is a Web browser designed primarily for mobile phones. Over the last few months, Opera Mini has gained in popularity as a mobile browser alternative on Android smartphones, becoming a target for cyber-criminals to trick users. In the latest attack, criminals offered the browser to users from a store other than Google's Play store. However, installing the application installed the actual Opera browser, and also a Trojan that sent SMS messages to premium-rate numbers.

Unlike other cases in which Trojans attempted to pass themselves off as popular mobile apps, in this case the malware came bundled with a legitimate version of the Opera Mini mobile browser to help trick users into thinking that nothing was wrong as they could simply use the real software as expected.


FIG.07. *CHINA MOBILE.*

We saw another 'unusual' attack in China, as a Trojan was released that purchased applications from the infected device. The Trojan affected Chinese subscribers to China Mobile, one of the world's largest mobile phone carriers with more than 600 million subscribers. Once infected, the mobile started buying applications from China Mobile's marketplace on behalf of the user. This Trojan was delivered on nine unofficial app stores.


FIG.08. *ANDROID.*

At this point, many users believe that it is safer to buy and install apps from official stores. This is true to some extent, but there have also been instances of malware creeping onto official stores. This quarter, for example, a new malware strain was discovered hiding out in the Google Play Android store, posing as two games: Super Mario Bros and GTA 3 Moscow City. The malware managed to remain undetected for weeks until it was finally removed.

Why is Android the most targeted mobile platform? Well, this is due to a number of reasons: Firstly, Android allows its users to get their apps from anywhere they want. They don't necessarily have to go to the official store, nor must applications be digitally signed as with iOS. Secondly, cyber-crooks would have never set their eyes on this platform if it weren't for the large number of users it has. In June, Google announced that 400 million Android devices had been activated, a figure that reached 500 million at the beginning of September, with 1.3 million activations per day.

# 03| Malware Figures in Q3 2012

In the third quarter of 2012 alone, more than six million new malware samples were detected by our laboratory, a similar figure to the first two quarters of the year. Trojans continued to account for most of the new threats, as three out of every four new malware strains created was a Trojan. Here are the details:

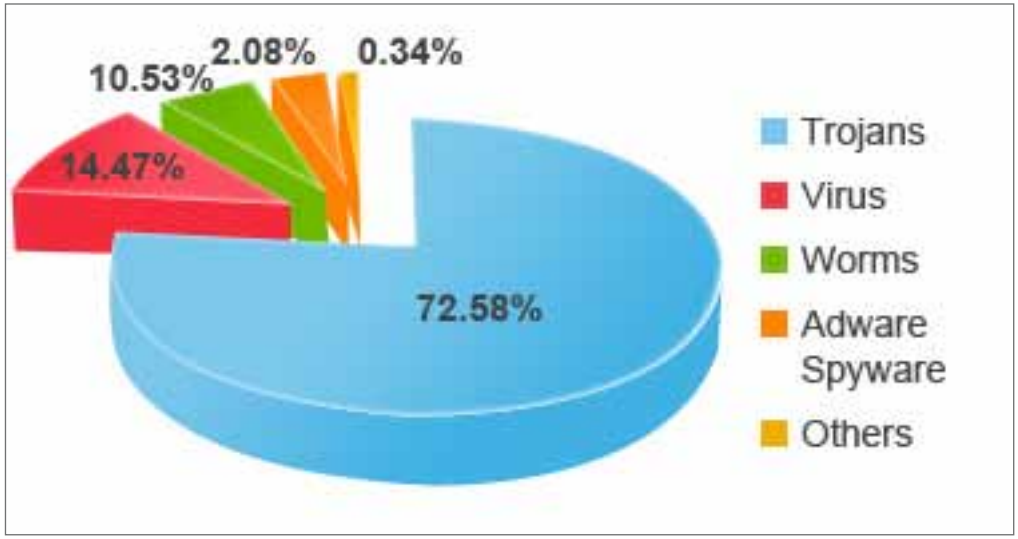


FIG.09. *NEW MALWARE CREATED IN Q3 2012, BY TYPE.*

When it comes to the number of infections caused by each malware category, Trojans once again topped the ranking, accounting for 78 percent of infections in Q3 according to our Collective Intelligence data. The graph below shows last quarter's distribution of malware infections:

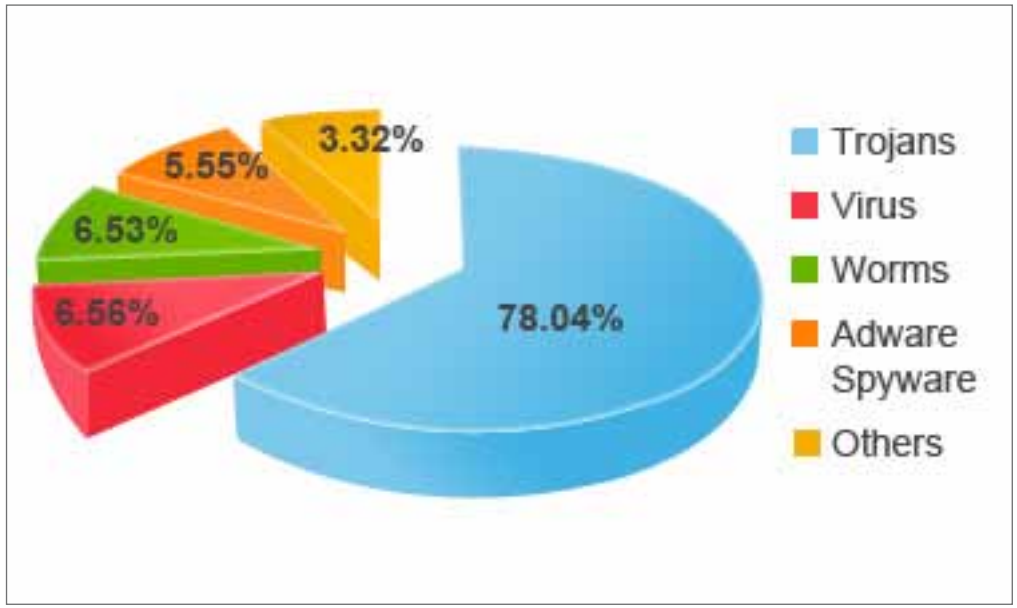


FIG.10. *MALWARE INFECTIONS BY TYPE IN Q3 2012.*

Data theft continues to be the main reason behind malware creation, as shown by the overwhelming proliferation of Trojans (78.04 percent of all samples detected by PandaLabs).

Let's now look at the geographic distribution of infections. Which countries were most infected? Which countries were best protected? The average number of infected PCs across the globe stood at 30.68 percent, slightly less than in Q2. Countries in Asia took the top two spots of most infections per country, with China leading the way (53.17 percent of infected PCs), followed by South Korea (52.77 percent). These two were the only countries whose infection rates exceeded 50 percent. Next came Turkey (42.51 percent).

The graph below shows the ten countries with the most malware infections in Q3 2012:

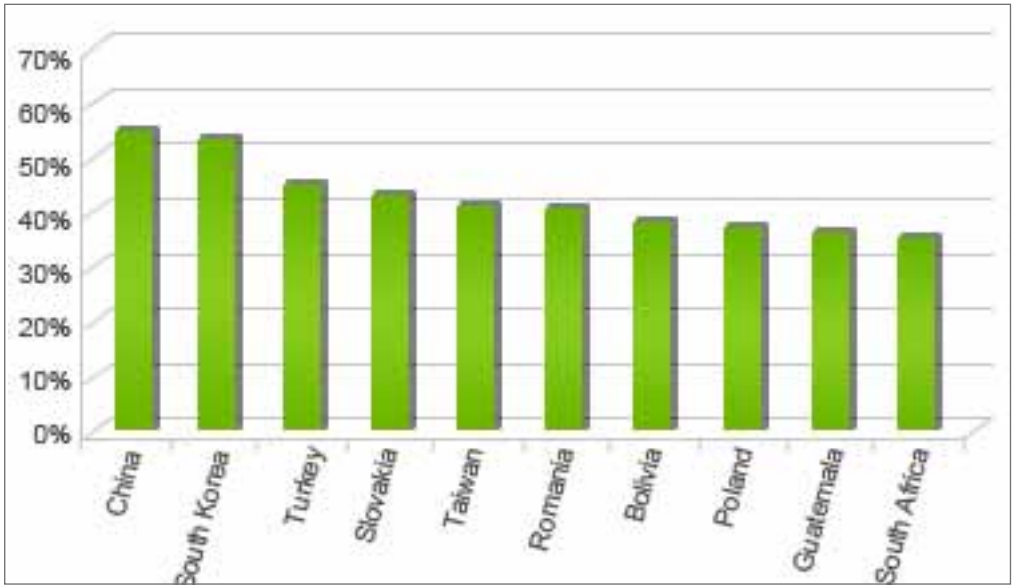


FIG.11. *MOST MALWARE INFECTED COUNTRIES.*

As the table shows, there are high-infection countries in almost every part of the world: Asia, Europe, South America, and Africa as well. Eight of the ten least infected countries are in Europe with the only exception being Canada and Australia. The country with the fewest infections is Ireland (20 percent of infected PCs), closely followed by Norway (20.16 percent). Sweden takes the third spot (22.46 percent), maintaining its presence as one of the countries least affected by malware infections over the last few yeas.

The graph below shows the ten countries with the fewest malware infections in Q3 2012:

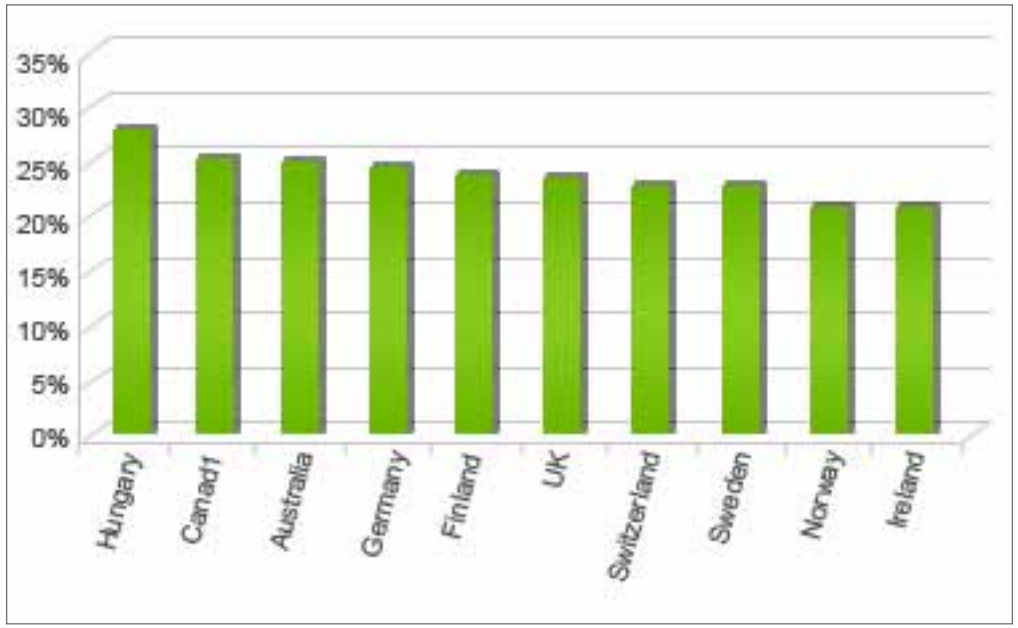


FIG.12. *LEAST MALWARE INFECTED COUNTRIES.*

# 04| Conclusion

This quarter we have seen major companies fall victim to data theft attacks that have compromised not only corporate data but customer details as well. We'd like to be able to say that data theft is on the decrease but unfortunately we can't. Not only do attackers steal user data but, as seen in the Adobe hack attack, they are looking for new ways to infect users, like hacking into corporate servers to add legitimate digital signatures to their malware creations.

The year is not over yet, and we must continue fighting malware creators and cyber-crimes. Even though the number of threats has remained stable during the year, with approximately six million new strains appearing every quarter, that doesn't mean we can relax.

This has been our summary of the most important IT security news in the third quarter of 2012. Hopefully, our next report will contain more information on the fight against cyber-crime and less stories about data breaches in companies. For their own good and for everybody's good…

Our next quarterly report will include a summary of all the events that took place in 2012. Also, we'll look into our crystal ball and make some predictions about what to expect in 2013.

# 05| About PandaLabs

PandaLabs is Panda Security's anti-malware laboratory, and represents the company's nerve center for malware treatment:

- **PandaLabs** creates continually and in real-time the counter-measures necessary to protect Panda Security clients from all kind of malicious code on a global level.

- **PandaLabs** is in this way responsible for carrying out detailed scans of all kinds of malware, with the aim of improving the protection offered to Panda Security clients, as well as keeping the general public informed.

Likewise, PandaLabs maintains a constant state of vigilance, closely observing the various trends and developments taking place in the field of malware and security. Its aim is to warn and provide alerts on imminent dangers and threats, as well as to forecast future events.

- For further information about the last threats discovered, consult the PandaLabs blog at: **http://pandalabs.pandasecurity.com/**

# Follow us on the Web


**facebook**
https://www.facebook.com/PandaUSA

**twitter**
https://twitter.com/#!/Panda_Security

**google+**
http://www.gplus.to/pandasecurity

**youtube**
http://www.youtube.com/pandasecurity1

*This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Panda Security. © Panda Security 2012. All Rights Reserved.*


PANDA SECURITY