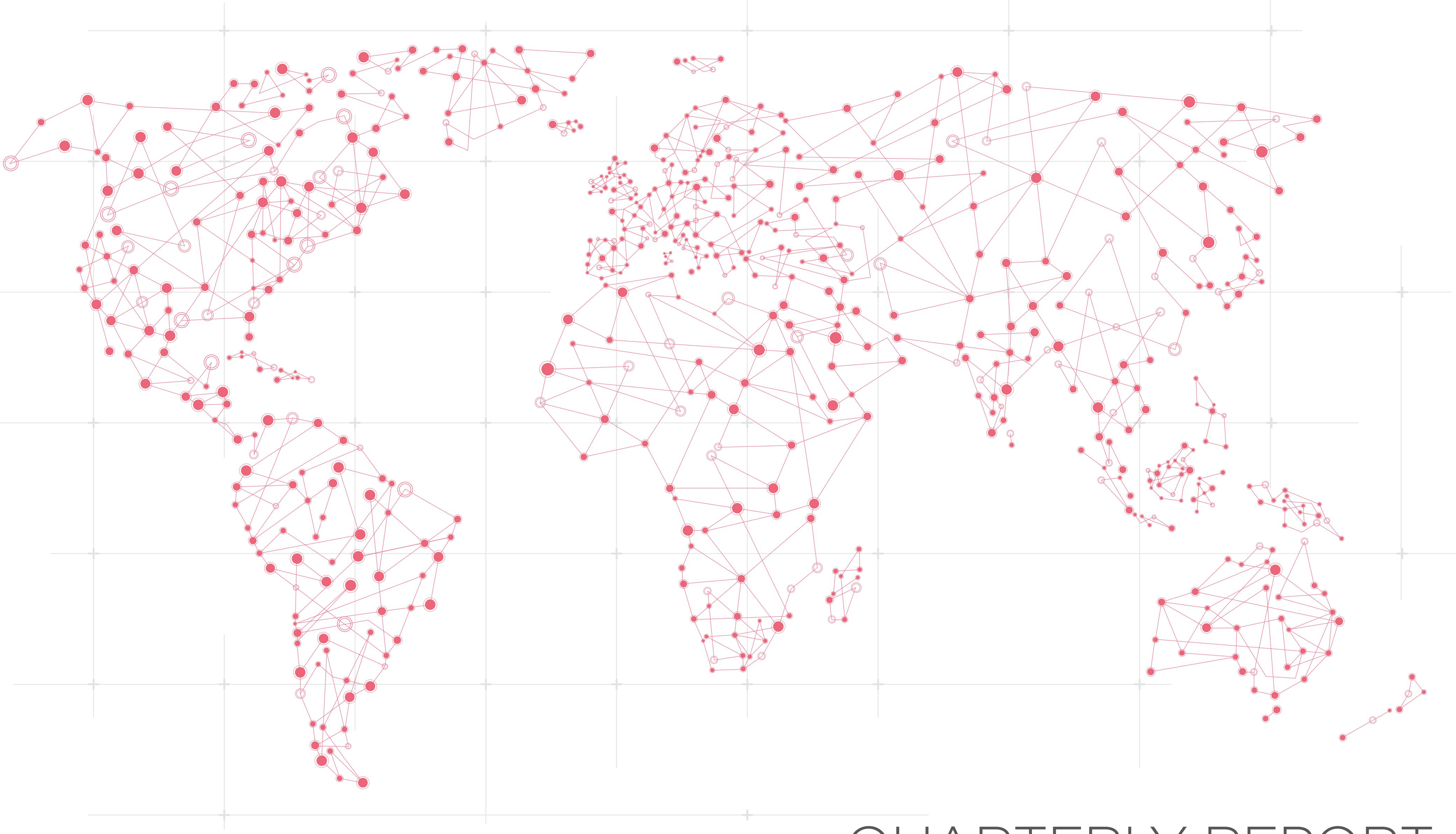
PANDALABS
THE EYE OF SECURITY



QUARTERLY REPORT

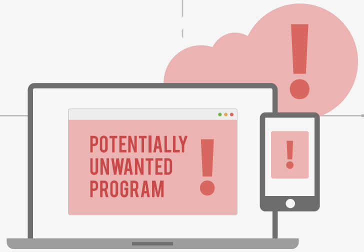
Q3 2014

PANDA SECURITY | The Cloud Security Company

INTRODUCTION

The third quarter of the year coincides with the summer vacation period and so it is often seen as a time to rest and relax… Well, not in the fight against cyber-crime. We haven't had a quiet time by any means and the number of cyber-attacks around the world has continued to grow exponentially.

__The number of brand new malware families created hit a record high, with more than 20 million new samples identified in the third quarter of the year.



The number of brand new malware families created hit a record high, with more than 20 million new samples identified in the third quarter of the year.

In the mobile malware area, while senior Android security engineers at Google proclaim that users don't have anything to worry about and antivirus programs may not be necessary for Android, new security flaws emerge that allow attackers to infect users' devices and take control of them.

We'll take a look at the #celebgate hack that leaked private photos of more than 100 actresses and models to the Internet, and Apple's responsibility in the attack. We'll also cover some of the massive data breaches suffered by companies around the world, including UPS, JP Morgan Chase, Home Depot, etc.

Finally, we'll turn our attention to the latest cyber-espionage scandals revealed by the documents leaked by former NSA employee Edward Snowden.

MALWARE FIGURES IN Q3

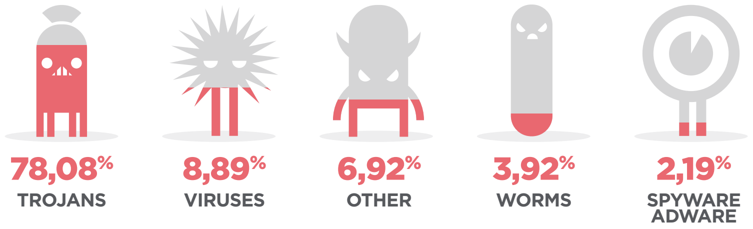
The amount of new malware in circulation rose significantly during the first half of the year, doubling last year's figure and reaching an average of 160,000 new samples created every day. And things got worse in Q3. At PandaLabs we recorded over 20 million new malware samples over the last three months, at an average of 227,747 new malicious items every single day.

The majority of these malware threats do not belong to new families developed from scratch, but are variants of well-known malware specimens conveniently modified by their creators to evade detection systems.

Trojans continued to be the most common type of malware, accounting for 78.08% of the new malware strains put in circulations, while traditional computer viruses came in second at a far-off 8.89%. This is a summary of the new malware appeared during this quarter:

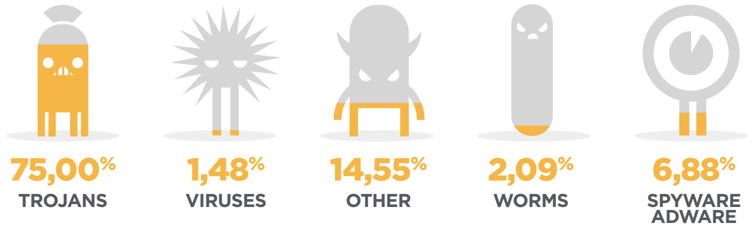
NUEVO MALWARE CREADO

NEW MALWARE CREATED IN THE THIRD QUARTER OF 2014, BY TYPE



If we analyze infections around the world, the figures are similar to those for new malware created. However, it must be noted that the infections caused by the malware included in the 'Other' category more than double the percentage of new malware created in the same category.

INFECTIONS BY TYPE OF MALWARE IN Q3 2014

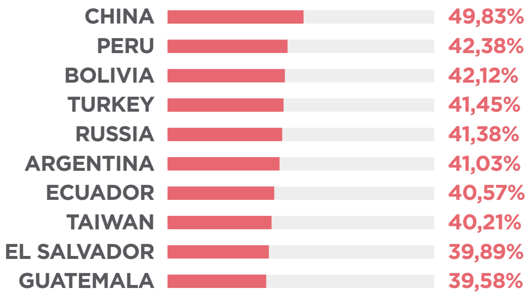


The malware included in the "Other" (which includes PUP - Potentially Unwanted Programs) and "Adware/Spyware" categories seems to be particularly efficient, as these specimens are capable of infecting proportionately more computers with fewer samples. This is mostly legal software that uses very aggressive means to reach computers, from bundling with free applications to using installers that distribute legitimate software but install other types of applications on users' computers without their consent.

The global infection rate was 37.93%, slightly up on recent quarters. Regarding the data across different countries, China is once again in pole position, with an infection rate of 49.83%. This is the first time in a long time that the Asian country has an infection ratio below 50%. China is followed by Bolivia (42.12%) and Peru (42.38%).

Below we list the 10 countries with the highest infection ratios:

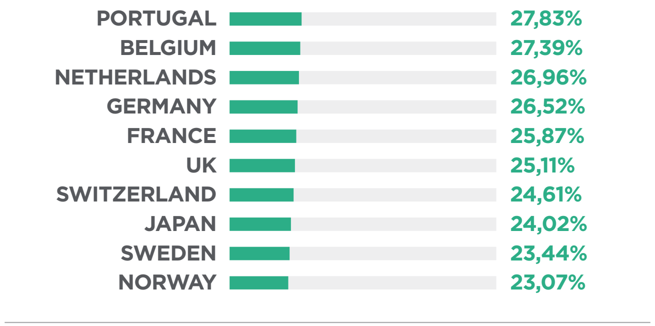
COUNTRIES WITH THE HIGHEST INFECTION RATES



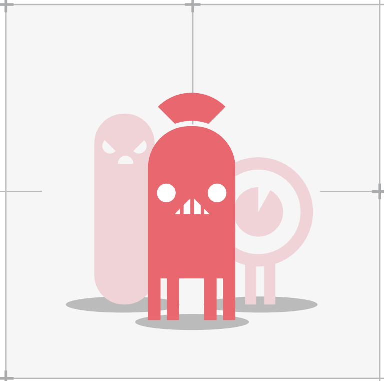
It's clear that the highest positions in the ranking are held by Asian and Latin American countries. Other countries with rates above the global average include: Poland (39.48%), Brazil (39.21%), Slovenia (39.05%), Colombia (38.86%), Spain (38.37%), Costa Rica (38.19%), Chile (38.05%) and Italy (37.97%).

In contrast, below is a list of the countries with the least infections:

COUNTRIES WITH THE LOWEST INFECTION RATES

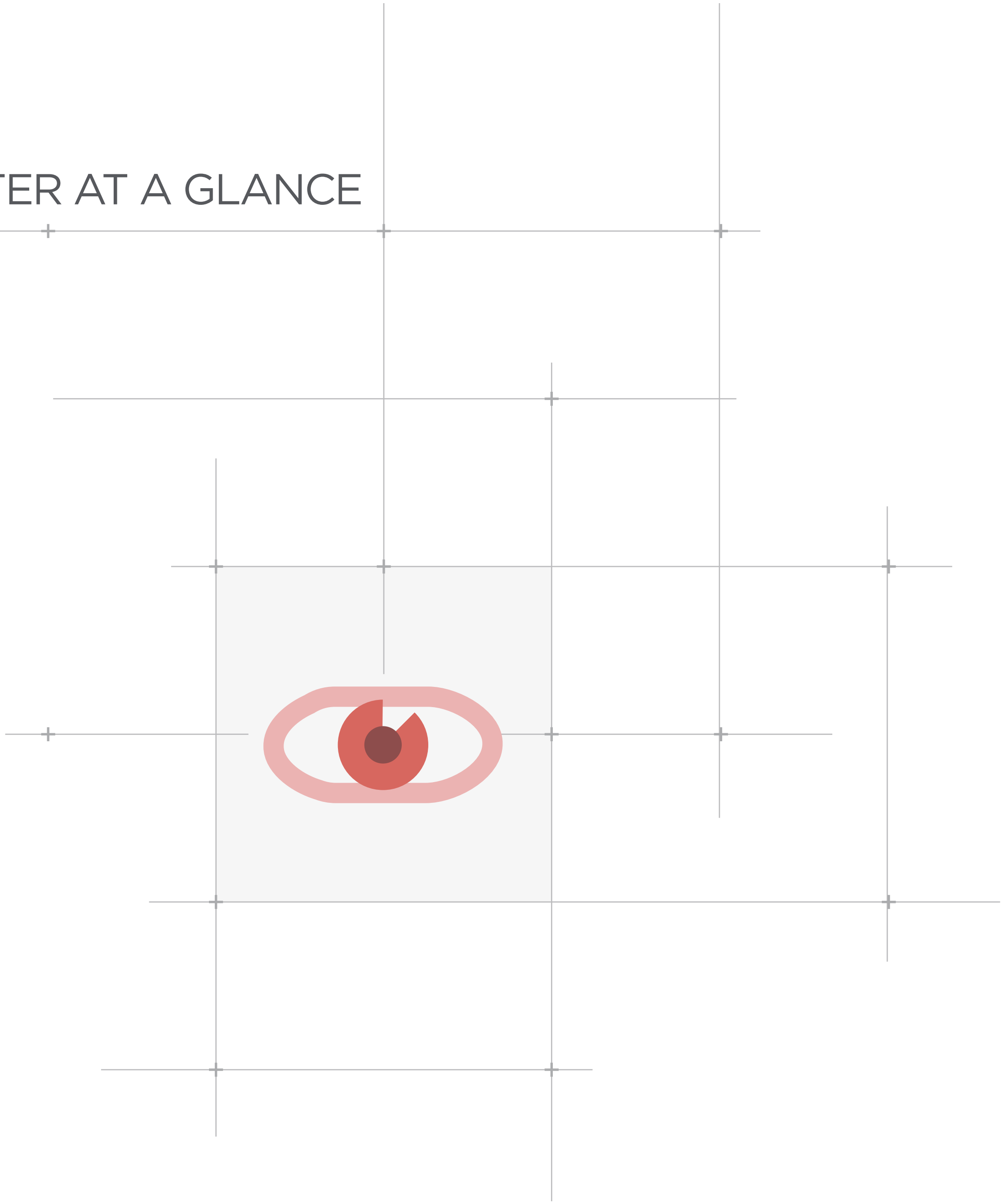


Europe in general is the area with the lowest infection rates and nine European countries figure in this ranking. Norway (23.07%), Sweden (23.44%) and Japan (24.02%) are the countries with least infections worldwide. Other countries which, although they haven't made the Top 10, are still below the worldwide average include: Denmark (28.18%), Finland (28.59%), Panama (29.77%), Canada (30.03%), Austria (30.55%), Uruguay (31.15%), Venezuela (32.35%), Australia (32.54%), USA (33.03%), Czech Rep. (34.46%), Mexico (36.31%) and Hungary (36.99%).



THE QUARTER AT A GLANCE

Despite coinciding with the summer season, the third quarter of the year was as busy as always. Below we summarize some of the major events that took place in the computer security world during that period.



CYBER-CRIME

__ iCloud was at the center of the much-discussed #celebgate scandal. This hacking attack leaked private photos of more than 100 actresses and models to the Internet. __

One of the best ways to mitigate hacking risks is to use two-factor authentication. Most major

online service companies (Facebook, Google, Microsoft, etc.) already have it, and this quarter, Apple, which already utilized two-factor authentication in its iCloud services, extended the feature to its iCloud.com Web app suite, providing users who access their iCloud accounts from their iPhones or iPads with an extra layer of security.

iCloud was at the center of the much-discussed #celebgate scandal. This hacking attack leaked private photos of more than 100 actresses and models to the Internet. Actresses such as Jennifer Lawrence, Kirsten Dunst or Kate Upton were among the victims of the mass photo hack, and the stolen images were obtained via the online storage offered by Apple's iCloud platform.

Initially it was thought that the leaks could be due to a potential security hole in iCloud, but Apple announced that, after a 40-hour investigation, they had discovered that the accounts of these celebrities "were compromised by an attack on the very specific user names, passwords, and security questions," adding that these attacks have "become all too common on the Internet."

Obviously, the culprits of this type of hack are always the attackers who steal the victims' photos, however, there are also lessons to be learned:

- Never upload images that you don't want to share.
- Enable two-factor authentication in your online accounts.

A Russian hacker group that goes by the name of w0rm attacked technology news website CNET and stole user names, emails and encrypted passwords of over a million users. This is the same gang that claimed responsibility for hacking the BBC, Adobe and Bank of America websites in the past.

The third quarter of the year saw massive data thefts at major companies and institutions around the world. Community Health Systems, one of the biggest U.S. hospital groups, announced that its computer network had been the target of a cyber-attack which saw the compromise of patient identification data for 4.5 million individuals. In August, grocery store chain Supervalu announced that attackers had managed to compromise customer data at 180 of its stores around the country. Additionally, UPS acknowledged that credit and debit card information belonging to customers who did business at 51 of its offices had been compromised as the result of an intrusion into the company's networks.

U.S. bank JP Morgan Chase fell victim to a similar data breach. Hackers launched targeted attack at specific JP Morgan Chase employees to gain access to their computers, and from there to the bank databases. The attackers modified and deleted some of the bank records yet the motive for these actions is unknown. Both the FBI and the Secret Service are investigating the case.

Home Depot was the victim of one of the largest attacks recorded this quarter. The home improvement retailer confirmed that its servers had been attacked and that 56 million credit and debit card details had been compromised. According to The Wall Street Journal, the company also acknowledged that, in some cases, the accounts associated to the cards were drained.

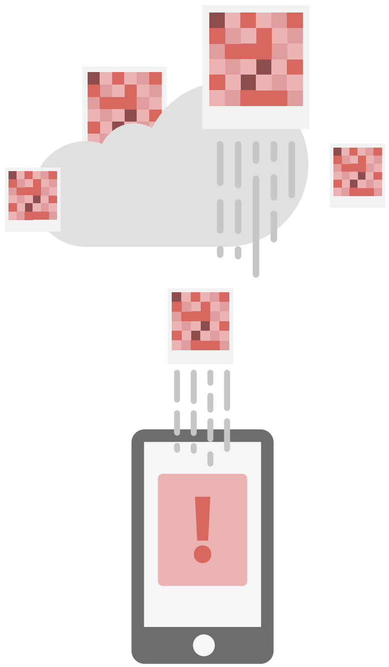
In addition, fraudulent transactions appeared across the USA as the criminals used the stolen card details to buy prepaid cards, electronic goods and even groceries.

This attack came just months after a similar attack on Target Corp., and there could be a connection, as the same tool –BlackPOS– was used to carry out the hack. It appears that the security breach may have affected customers who shopped in any of the almost 4,000 stores that the company has in the U.S. and Canada between April and September.

The news of a potential hack attack on Google hit the headlines after a list of almost five million Gmail user names and passwords was leaked online. In a statement sent to the media, Google said it had no evidence that its systems had been compromised, adding that whenever they become aware that accounts may have been compromised, they take steps to help users secure their accounts. Google said that 98% of the passwords did not work, and the leaked data seems to have been accumulated through phishing and other hacking attacks on users.

A security hole was discovered in Bash that jeopardized the security of Linux and Mac users. This vulnerability, dubbed 'Shellshock', affected the command interpreter in these operating systems. This flaw could allow a cyber-criminal to remotely access a system using Bash and insert spyware designed to steal confidential information or even take control of the system.

The affected systems include Mac OS X computers, many Web servers, and some home networking devices like routers.



SOCIAL NETWORKS

__ Twitter joins the group of companies that reward the efforts of those users who dedicate to uncover security holes in their programs or platforms.__

In the technology world, it is now quite common for companies to reward the efforts of those advanced users who dedicate some of their time to uncovering security holes in their programs or platforms.

Although there are still some who are yet to be convinced of the effectiveness of such 'bounty programs', many firms apparently see them as being extremely useful, not just to discover new bugs that have gone undetected, but also to get these expert users on their side. Twitter was still among those that had yet to take up the idea. The 140-character social network seemed reluctant to put its hand in its pocket to encourage experts to find bugs in its service.

Nevertheless, now the company has announced that it is offering a minimum reward of $140 for those who find security holes in Twitter.com, ads.twitter, mobile Twitter, TweetDeck, apps.twitter, as well as in the apps for iOS and Android. This sum is still way off what others are offering. Bounty programs at firms like Facebook or Google reward users that uncover vulnerabilities with amounts upwards of $500 and $1,000 respectively.

Mobile Malware

__ Android malware has continued to grow exponentially, and 2014 is already the year in which most mobile malware strains have been put in circulation. __

Android was once again the main target for mobile malware creators. Adrian Ludwig, the lead security engineer for Android at Google, said there was "a bit of misperception" in how the company review apps for its Google Play store in comparison with other stores (a not-so-subtle swipe at Apple's iOS App Store, which has a reputation of being much more demanding in this respect). In this context, he even proclaimed that mobile antivirus was not needed on Android.

Android malware, meanwhile, has continued to grow exponentially, and 2014 is already the year in which most mobile malware strains have been put in circulation.

Additionally, new vulnerabilities have emerged that could be exploited by attackers for malicious purposes:

- CVE-2013-6272: Exists in all Android versions through 4.4.2 (KitKat). It allows applications to make unauthorized calls to premium-rate telephone numbers.

- CVE-2014-N/A: Exists in Android 2.3.3 and 2.3.6, and has the same effect as the previous one.

CYBER-WAR

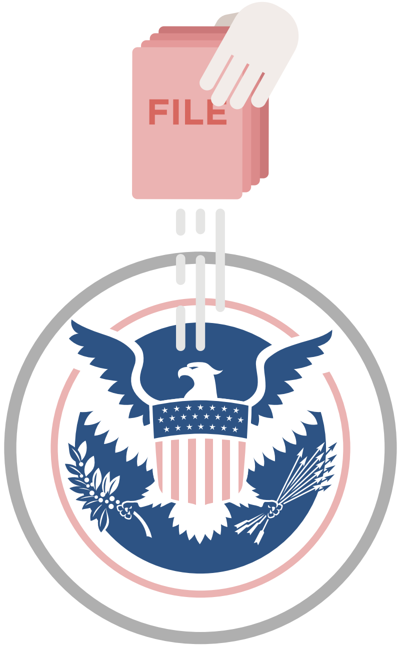
In July, U.S. newspaper The New York Times revealed that alleged Chinese hackers had gained access to some of the databases managed by the Office of Personnel Management to house the personal information of the federal employees who apply for top-secret security clearances. The U.S. Government acknowledged the attack but denied the possibility that any classified information had been compromised. Despite the attackers were tracked back to China, there is no conclusive proof that they were working on behalf of the Chinese government.

__The third quarter of the year saw massive data thefts at major companies and institutions around the world. __

In the cyber-espionage arena, top-secret documents from the NSA and the British agency GHCQ revealed the existence of "Treasure Map", a secret operation aimed at mapping the entire Internet, including end-user devices. The documents leaked by former intelligence service employee Edward Snowden revealed how the NSA and its intelligence partners had illegally penetrated the internal networks of different companies in order to fulfill their objective. One of these companies is German firm Deutsche Telecomm which, after been alerted to the possibility of this attack by German magazine Der Spiegel, scanned its network without being able to find any evidence of intrusion.

Other classified documents revealed by Snowden showed how British intelligence agency GHCQ had the ability to actively monitor Skype users in real time without their knowledge.

In August, a hacker claimed to have stolen 40 GB of internal documentation from Gamma International (http://en.wikipedia.org/wiki/FinFisher), a German-UK technology company that develops spying software for governments and police agencies around the world. The attacker created a Twitter account (@GammaGroupPR) through which he began posting links to the stolen documentation.

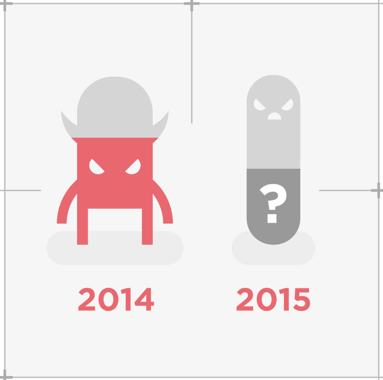


CONCLUSION

The third quarter of 2014 was as exciting as expected. In fact, we recorded the highest number of new malware specimens in history, and saw some of the largest data breach cases to date, with millions of credit card and personal details stolen.

Judging by the frantic activity that has marked the year so far, there is no doubt that the last quarter of 2014 will be equally exciting. Will malware creation continue to grow or will it finally slow down? What new tactics can we expect to see in the mobile realm? What new companies will fall victim to cyber-attacks? What new documents will Edward Snowden leak and how will they affect the already tarnished reputation of the NSA?

You'll find the answers to these questions and many more in our next report, which will offer a summary of the most significant events that occurred during the year, as well as a forecast of next year's cyber-security threats.



ABOUT PANDA**LABS**

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.

f https://www.facebook.com/PandaSecurity

https://twitter.com/PandaComunica

g+ https://plus.google.com

You Tube http://www.youtube.com/pandasecurity

in http://www.linkedin.com/company/panda-security

http://mediacenter.pandasecurity.com

PANDALABS
THE EYE OF SECURITY