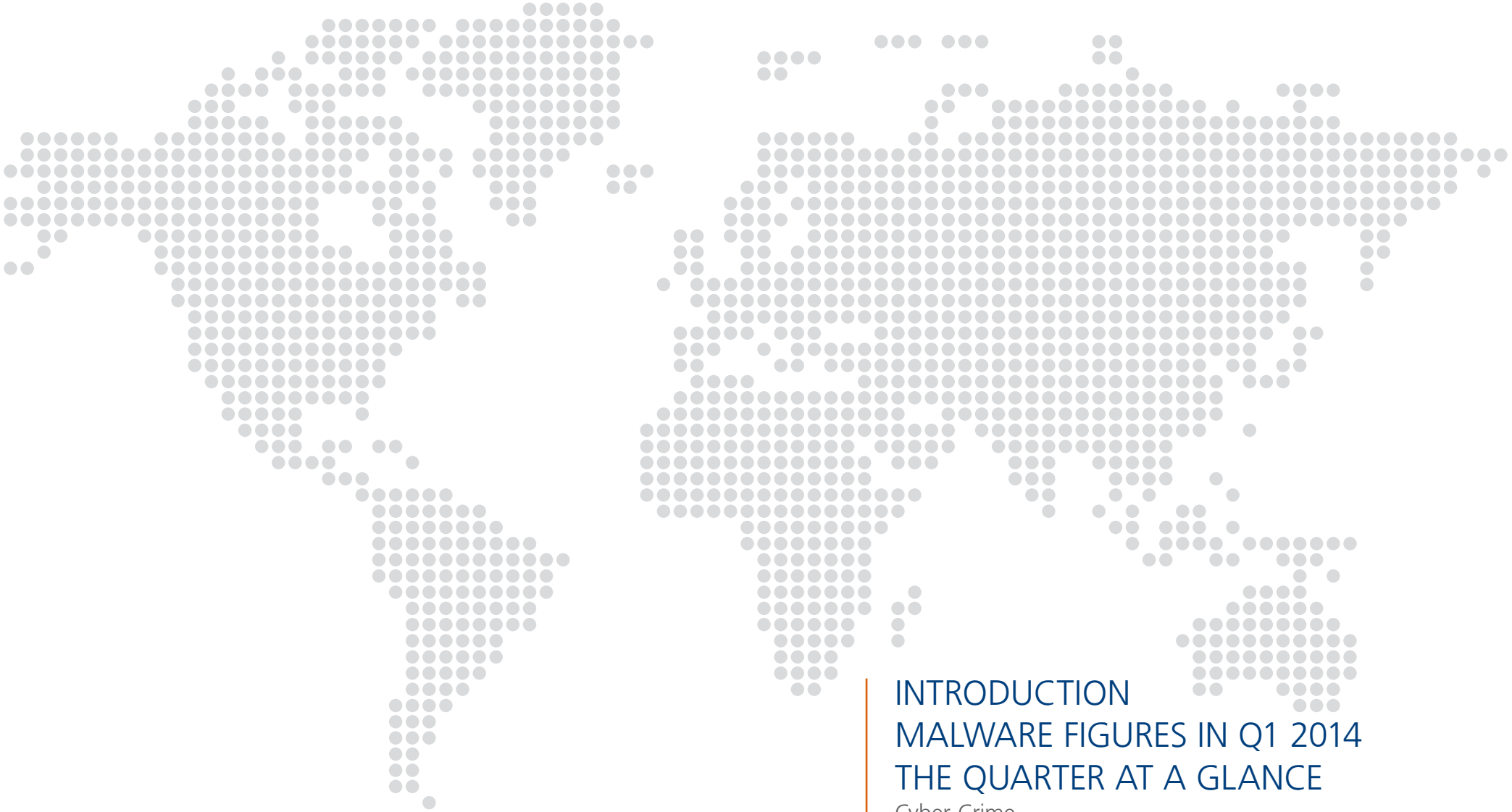
PANDALABS

THE EYE OF SECURITY

QUARTERLY REPORT

JANUARY-MARCH 2014



CONTENTS

INTRODUCTION

We've just finished the first quarter of what promises to be an exciting year in the computer security field. In our first report of 2014 we'll take a look at the malware statistics compiled by PandaLabs, which illustrate how cyber-criminal activity continues to increase as malware creation hits record levels. Also, we'll summarize the latest data breaches occurred around the world, some of the biggest ever, with millions of affected users.

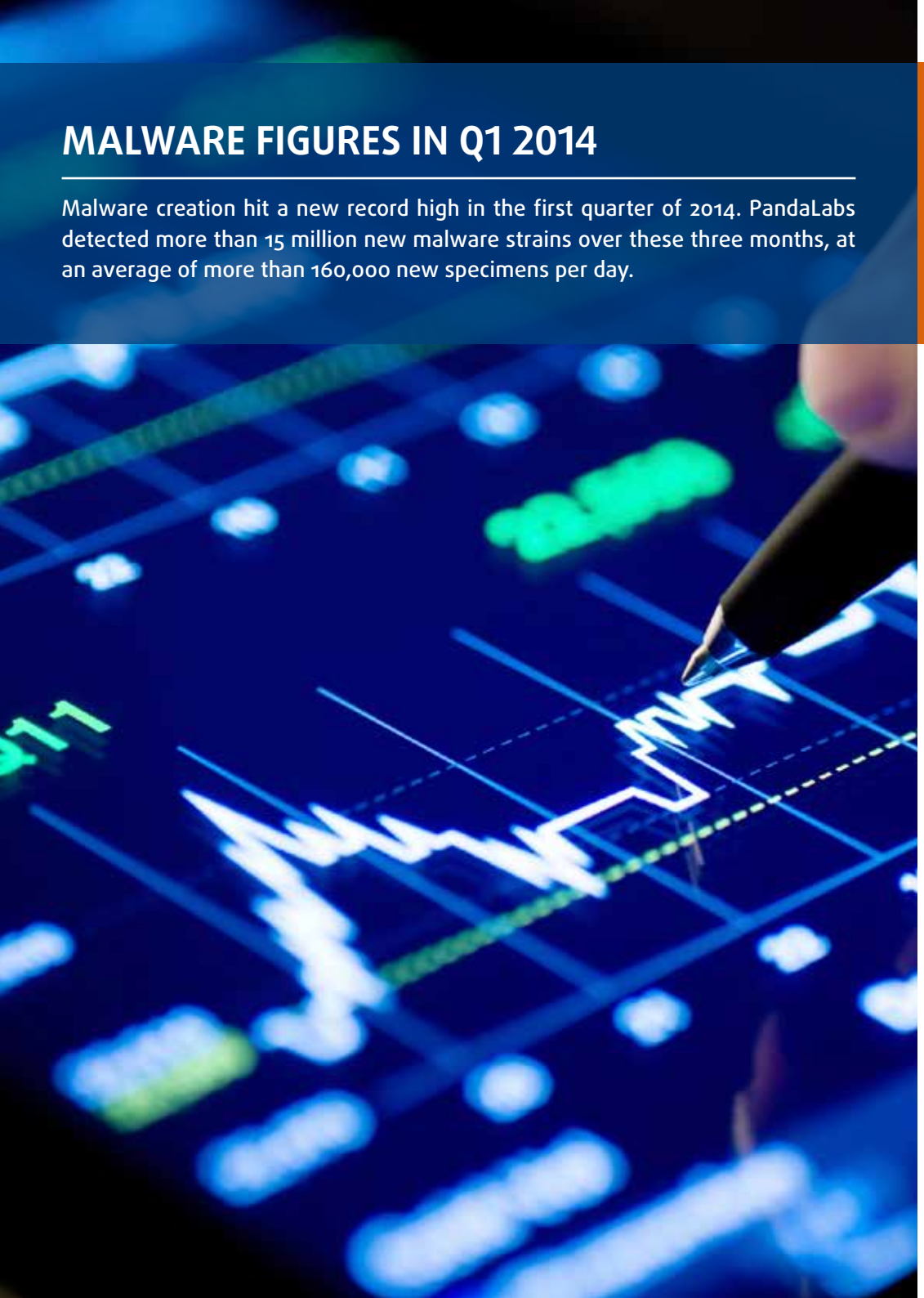
In the mobile malware arena, Android was the target of various attacks designed to subscribe users to premium SMS services via malware apps on Google Play and malicious advertising on Facebook using WhatsApp as bait.

We'll discuss the latest activities of the Syrian Electronic Army hacking collective, whose victims included big companies such as Microsoft or Facebook (albeit without success in the latter case).

Finally, in the cyber-espionage world, we will analyze the latest news regarding the operations conducted by the NSA and British intelligence agency GCHQ (Government Communications Headquarters), with special attention to the controversy surrounding the "Optic Nerve" surveillance program run by both agencies to indiscriminately spy on millions of users through their own webcams.

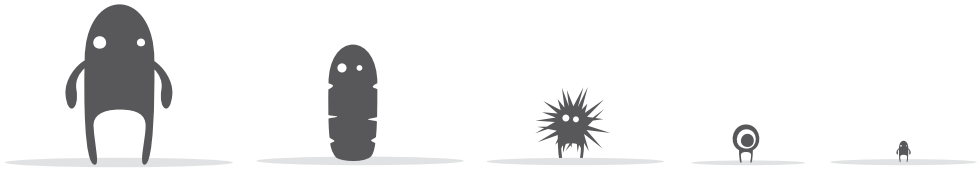
MALWARE FIGURES IN Q1 2014

Malware creation hit a new record high in the first quarter of 2014. PandaLabs detected more than 15 million new malware strains over these three months, at an average of more than 160,000 new specimens per day.



Trojans continued to be the most common malware threat, accounting for 71.85% of all new malware created. This figure is very similar to the previous quarter.

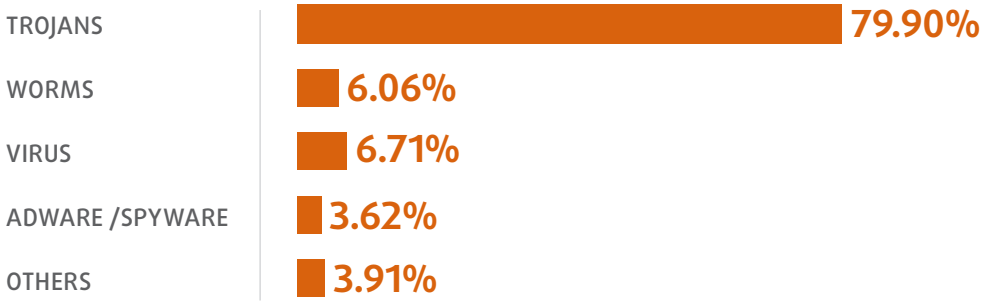
NEW MALWARE STRAINS IN Q1 2014, BY TYPE



71.85%	12.25%	10.45%	5.26%	0.19%
TROJANS	WORMS	VIRUSES	ADWARE SPYWARE	OTHERS

Analyzing all infections around the world, the numbers are similar to those for the new malware samples created:

MALWARE INFECTIONS BY TYPE IN Q1 2014

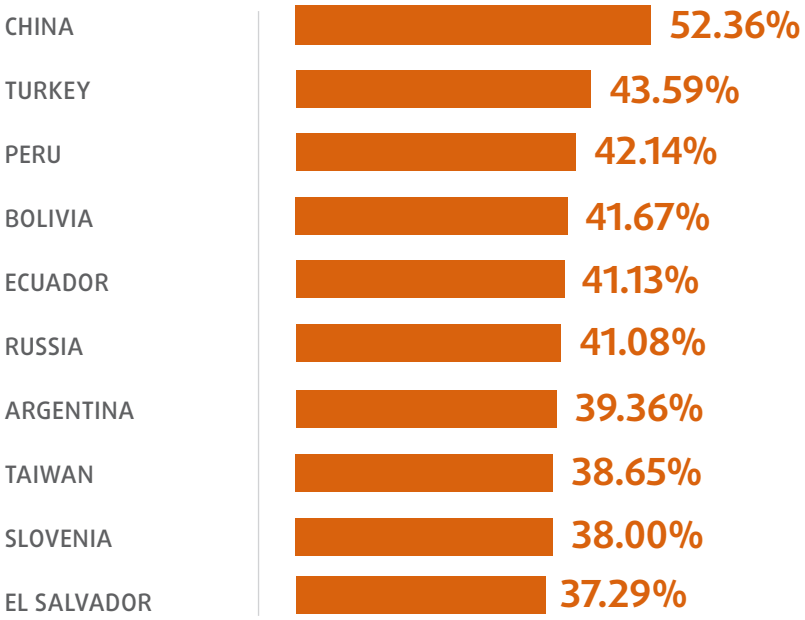


Trojan infections top the ranking as the weapon of choice for malware writers to infect users (4 out of every 5 computer infections were caused by Trojans).

We will now look at how infections were distributed geographically. In the first quarter of 2014, the global infection rate was 32.77%, which was up on the last few quarters. As for the data for individual countries, **China once again tops the table** with an infection rate of 52.36%, followed by Turkey (43.59%) and Peru (42.14%).

The graph below shows the ten countries with the most malware infections during the first quarter:

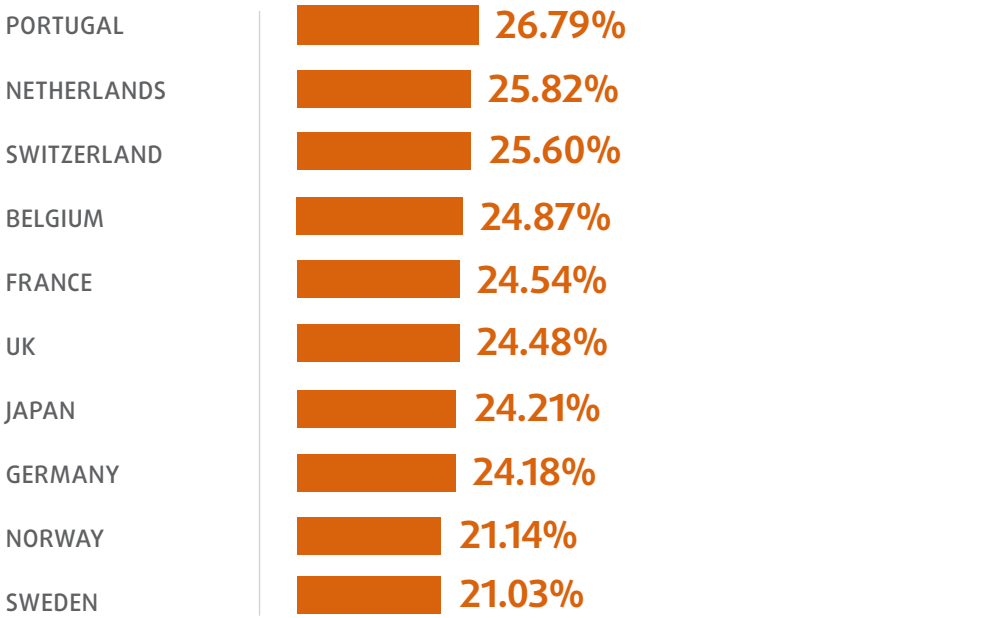
MOST MALWARE-INFECTED COUNTRIES



In this "Top 10", although there are countries from many regions, there is a strong presence of Asian and Latin American countries. **China is the only country in the world with an infection rate over 50%**. In addition, the following countries have an infection rate over the global average: Brazil (35.83%), Poland (35.59%), Guatemala (35.51%), Colombia (33.86%), Spain (33.57%), Costa Rica (33.33%) and Chile (33.22%).

Below you can see the countries with the fewest infections:

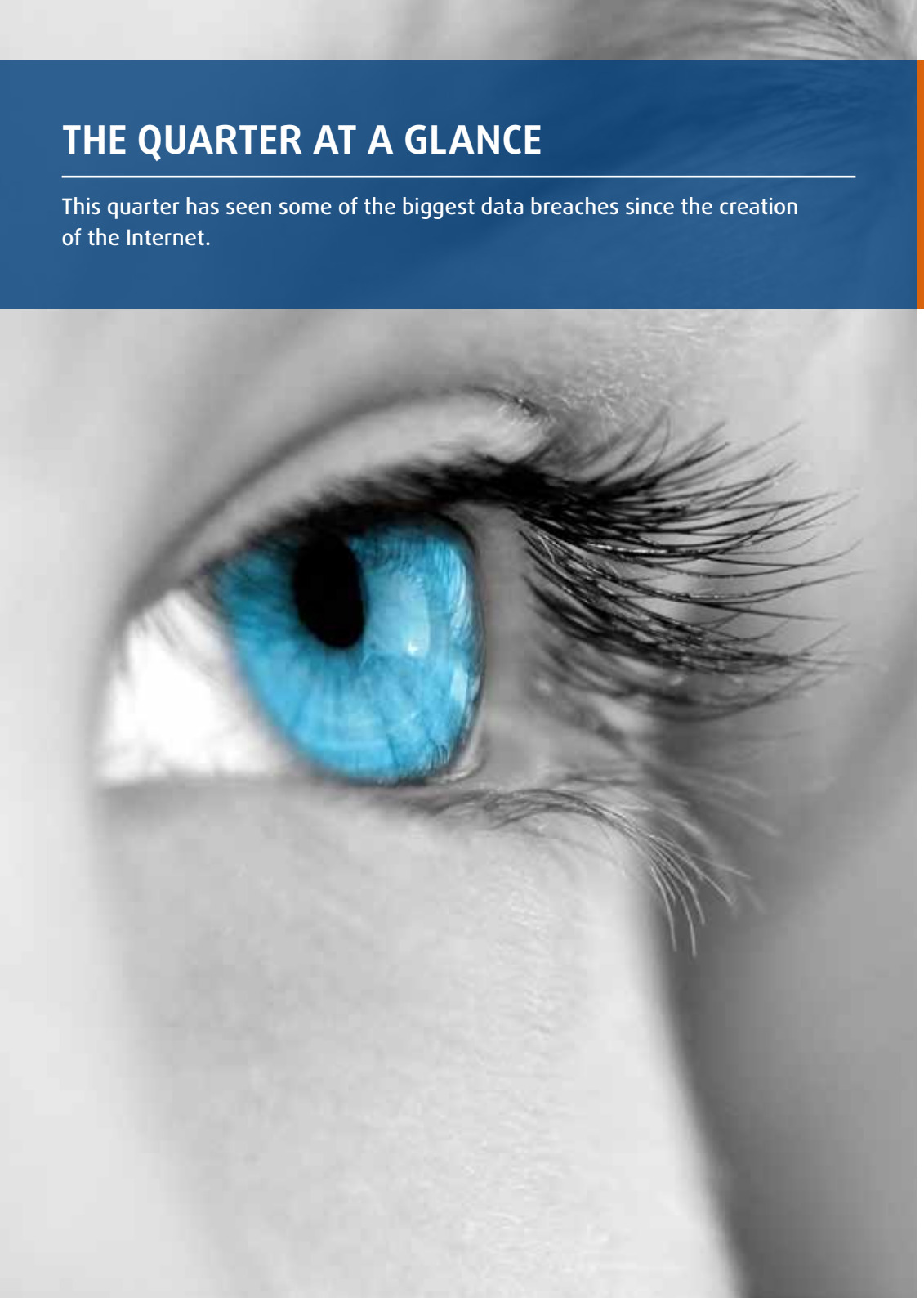
LEAST MALWARE-INFECTED COUNTRIES



Europe continues to have the lowest infection rates, with nine European countries occupying the top 10 positions in the ranking. Sweden (21.03%), Norway (21.14%) and Germany (25.18%) are the countries with the lowest infection rates. **The only non-European country in the Top Ten was Japan**, in fourth place with 24.21%. Other countries outside this Top 10 but with infection rates below the average are: Denmark (27.08%), Finland (27.16%), Panama (27.52%), Canada (27.54%), Austria (28.74%), Uruguay (28.89%), Venezuela (30.11%), Australia (30.45%), USA (31.16%), Czech Rep. (31.58%), Mexico (32.35%) and Hungary (32.74%).

THE QUARTER AT A GLANCE

This quarter has seen some of the biggest data breaches since the creation of the Internet.



CYBER-CRIME

At the end of last year, US retailer **Target** reported that hackers had stolen the credit and debit card details of some 40 million in-store shoppers. In this case, the breach did not affect online shoppers but customers who purchased products at the **company's stores** and paid with their credit cards. And not only was this information stolen but it was immediately sold on the black market.

Target Corp suffered a data breach compromising the credit and debit card details of 40 million in-store shopperss

At the beginning of the year new details emerged about the attack.

According to information leaked to Brian Krebs, one of the company's Web servers was compromised. From there, a Trojan was distributed to Target's point-of-sale terminals.

The malware was specifically designed for point-of-sale systems and stole the credit card data directly from the card readers' RAM. The attackers then accessed the compromised server in Target's internal network to collect the information captured from the infected terminals.

How can companies protect themselves from this type of attack? Antivirus solutions in this case are not the answer, as we are dealing with targeted attacks where the malware strain is specifically customized to avoid detection by the antivirus software in use.

As point-of-sale systems are usually closed platforms, you could think that a whitelisting solution would be extremely effective in such an environment. Whitelisting solutions are designed to lock down a machine so that only certain trusted applications are allowed to run, whereas everything else is denied. This could be a very effective means of neutralizing internal attacks in which, for example, an employee tried to infect a terminal by planting some type of malicious software in it. However, whitelisting doesn't provide a universal solution. On many occasions malicious applications are installed by exploiting system vulnerabilities, and this is not necessarily detected by whitelisting programs.

Point-of-sale terminals are a highly prized target for criminals. Today it is not a question of 'if', but rather 'when' they will be attacked, that's why businesses need security solutions that are able to:

- Restrict software execution. Only trusted processes must be permitted to run.
- Identifity vulnerable applications, warning of any software that requires updating.
- Control the behavior of allowed processes , should there be an attempt to exploit a vulnerability in a trusted process.
- Traceability. If an incident occurs, the solution must offer as much information as possible in order to answer four basic questions: when did the intrusion occur, which users have been affected, what data has been accessed and what has been done with it, as well as knowing how and where the attack was launched from.

These are not all the security measures that could be implemented, but the four most important points to observe when securing a system.

If the Target data breach was huge, South Korea witnessed one of the largest ever cyber-security attacks. Credit ratings agency Korean Credit Bureau (**KCB**) was the victim of a cyber-attack that resulted in the theft of personal financial information from 105.8 million banking accounts. The stolen information included credit card numbers, names, phone numbers, home and email addresses and even passport numbers. If you take into account that South Koreans on average have 5 credit cards, it means that at least 21 million users may have fallen victim to the attack, approximately 42 percent of the country's total population. In fact, the number of actual victims will probably be larger as not all users will have had all of their credits cards compromised. In this context, it may be harder to find people not affected by the data theft than the other way round.

Unlike the cyber-attack on Target, this time the criminals didn't use a particular strain of malware to steal the information. The theft appears to be the an inside job by a KCB worker –ironically enough, working at the company's anti-fraud department– who copied this information over a period of 11 months with the intention of selling it later to the highest bidder. The fact that the information stored by the company was not properly encrypted adds to the severity of the data breach. And the fact that an employee was able to steal information for more than 11 months also speaks volumes about the lack of proper supervision and access control mechanisms.

Nearly half the people in South Korea had their bank details stolen by a Korean Credit Bureau worker

There are a number of security measures that could have been implemented to prevent a situation like that, despite the fact that the thief in this case was a member of the company's anti-fraud department, and as such had access to sensitive information. What could have been done to prevent it? Well, as previously said, data encryption can be useful in situations like this, even thought the attacker in this case may very well have had access to the data needed to decrypt the information. Also, limiting the amount of information that can be accessed at a time can reduce the damage done by this type of data breach: If the attacker had been able to only access a limited number of records in the database –let's say, 10 records for example– he would have had to repeat the same operation more than 10 million times to achieve the same result. And not only that, you can also limit the amount of data that can be accessed over a period of time, and better still: You can set alerts linked to a series of complex rules that trigger whenever some unusual activity takes place. This is something most financial institutions have already implemented, allowing them to detect cyber-fraud and data theft.

The first quarter of 2014 also also saw other, less notorious data theft attacks. For example, in Germany, the Federal Office for Information Security (BSI) released a statement saying that around 16 million email accounts had been stolen. In this case the criminals used a botnet to perpetrate the attack, which means that most probably the victims' computers had become part of a computer network controlled by the hackers.

Germany's Federal Office for Information Security revealed a data breach where 16 million email addresses were stolen

The **BSI** created a website to help people find out whether or not their email account had been hacked. If you are among those affected, it is very likely that your computer is infected with malware. In that case, we advise that you use Panda Cloud Cleaner, a free tool that will allow you to scan your computer and remove malware threats.

Yahoo users were also affected by a security breach, although in this case the stolen data was not obtained directly Yahoo's servers. Apparently, some users of Yahoo email informed the company that their user IDs and passwords had been compromised, and after further research, it was discovered that the information had been obtained from a third-party database.

In response to the attack, Yahoo reset the victims' passwords and used two-factor authentication to let users re-secure their accounts.

Unlike the Yahoo incident, an attack launched on **Orange** did affect one of the company's websites. More specifically, the breached site was affected by a vulnerability that allowed the attackers to gain access to personal data from hundreds of thousands of customers, including names, mailing addresses and phone numbers.

Orange confirmed hackers stole 800,000 customer records

Fortunately, it seems that Orange's systems were configured in a way that prevented the customers' passwords from being compromised, which limited the damage done to the more than 800,000 users affected by the attack. According to reports, the customers' passwords were stored on a separate server which was not impacted by the breach.

In any event, when it comes to protecting passwords from the eventuality of theft, the best policy is simply not to store them. If passwords are not stored, they can't be stolen, can they? It sounds quite obvious, but not many companies seem to apply this simple concept.

Now, the question is, if organizations don't store users' passwords, how can they validate users? Very simple. It would be enough to 'salt' the original password set by the user when signing up for a Web service, and apply a hash function to that 'salted' password. By salting the original password, what you actually do is generate a new, different password using a previously defined pattern (turn letters into numbers, change their order, etc). Next, the system applies the hash function to the alternate password and converts it into a complex string of symbols by means of an encryption algorithm. It is this 'hashed' form of the password which is stored in order to validate the user. From that moment on, every time the user types in a password, the system will apply the aforementioned pattern to it, calculate a hash value, and compare it to the hash stored in the password database. If they match, it means that the user has entered the correct password and access is permitted. As you can see, the entire process takes place without the need to store sensitive data such as passwords.

Another measure that should be implemented on a massive scale is the use of two-factor authentication. Even though it can be a pain at times, when applied, it makes compromising user accounts a lot more difficult. This is a system that financial institutions have been using for a long time, and which should also extend to other Web services as well.

The Syrian Electronic Army defaced Forbes' website, stealing more than 1 million user accounts

The hacker collective known as the **Syrian Electronic Army** (SEA) managed to hack into Forbes' website, successfully stealing details from more than 1 million user accounts, including those of hundreds of the company's employees. The stolen information included user names and email addresses as well as passwords (in encrypted form). To make things even worse, the SEA published this data online.

Cryptolocker, the notorious and dangerous ransomware that encrypts victims' files until a ransom is paid, struck again. One of its many victims was Goodson's law firm in North Carolina (USA), which admitted that every legal file on one of its main servers had fallen prey to the malware. Incidents like this highlight once again the importance of backup policies in business environments, as the damage done by data breaches such as this would be clearly mitigated with a backup copy that allowed organizations to restore their information easily.

Cryptolocker continued to create havoc: its many victims included a law firm in North Carolina whose entire cache of legal files was encrypted by the malware

When talking about cyber-attacks we normally think of computers, smartphones and tablets. However, other hardware devices can be affected as well, as shown during the first quarter of the year. A security flaw in Linksys routers could allow an attacker to perform actions such as changing the router's DNS settings -something quite usual in phishing attacks that redirect users to fake websites

Banking Trojans are one of the most prevalent threats today. They are designed to gain access to victims' bank accounts and empty them, which makes them particularly dangerous and one of cyber-criminals' preferred weapons. In January, the U.S. Department of Justice announced that Russian national Aleksandr Panin had pleaded guilty to conspiracy to commit wire and bank fraud for his role as primary developer and distributor of one of the worst banking Trojans ever: SpyEye.

Aleksandr Panin, the alleged mastermind behind the notorious SpyEye Trojan, pleaded guilty to bank fraud

SOCIAL NETWORKS

The world was shocked with the recent mysterious disappearance of Malaysia Airlines flight MH370. Shortly after the news about the missing plane broke, cyber-criminals started preying on people's morbid curiosity through fake Facebook postings promoting a video of the plane. However, when users tried to watch the video, they were asked to enter their user names and passwords, compromising their accounts. Shortly after, the attackers carried out the same strategy on Twitter.

Cyber-criminals exploited the disappearance of Malaysia Airlines flight MH370 to launch attacks via Facebook and Twitter

As well as on social networks, PandaLabs detected a malicious email message exploiting the same subject matter. The message claimed to contain a transcript of the conversations held between the pilots and the control tower in the final minutes before ground controllers lost contact with the aircraft. The malware was attached to an executable file with a PDF icon to trick users into running it. Once run, the file infected the computer with a Trojan while at the same time opening a document with the supposed transcript so as not to raise suspicion.

The **Syrian Electronic Army**, already mentioned in this report, was particularly active in the social media arena, compromising the accounts of major companies worldwide. Its victims included **Microsoft**, whose @XboxSupport and Microsoft News (@MSFTNews) Twitter accounts were hacked. However, these were not the only attacks suffered by the Redmond company. On January 1, Microsoft's Skype had their Twitter and Facebook accounts hacked by the same group.

Syrian Electronic Army compromised the Twitter and Facebook accounts of several organizations worldwide and attempted to gain control of the facebook.com domain in an attack stopped by MarkMonitor

Unfortunately, these were not the only attacks perpetrated by the SEA. Actually, they tried to hijack the entire Facebook domain. They were able to gain access to an administrator panel at DNS provider **MarkMonitor**, but fortunately enough the hack was detected as it was taking place and MarkMonitor was able to regain control of the domain before the SEA was able to modify the Facebook.com DNS records.

MOBILE MALWARE

In February, PandaLabs identified a number of malware apps on Google Play. Four apps (on subjects such as diet plans, hairstyles, workout routines and recipes) on the Google Play store were identified as subscribing users to a premium SMS service. Not only this, the SMS messages received were then hidden so that the victim was unaware that anything was wrong until they saw their phone bill.

PandaLabs identified four malicious apps on Google Play with somewhere between 300,000 and 1,200,000 downloads in a little bit more than one month

A few weeks later, PandaLabs detected a similar attack, although this time, instead of using Google Play, cyber-crooks created a fake Web page designed to look like it, and spread the malware through malicious ads on Facebook.

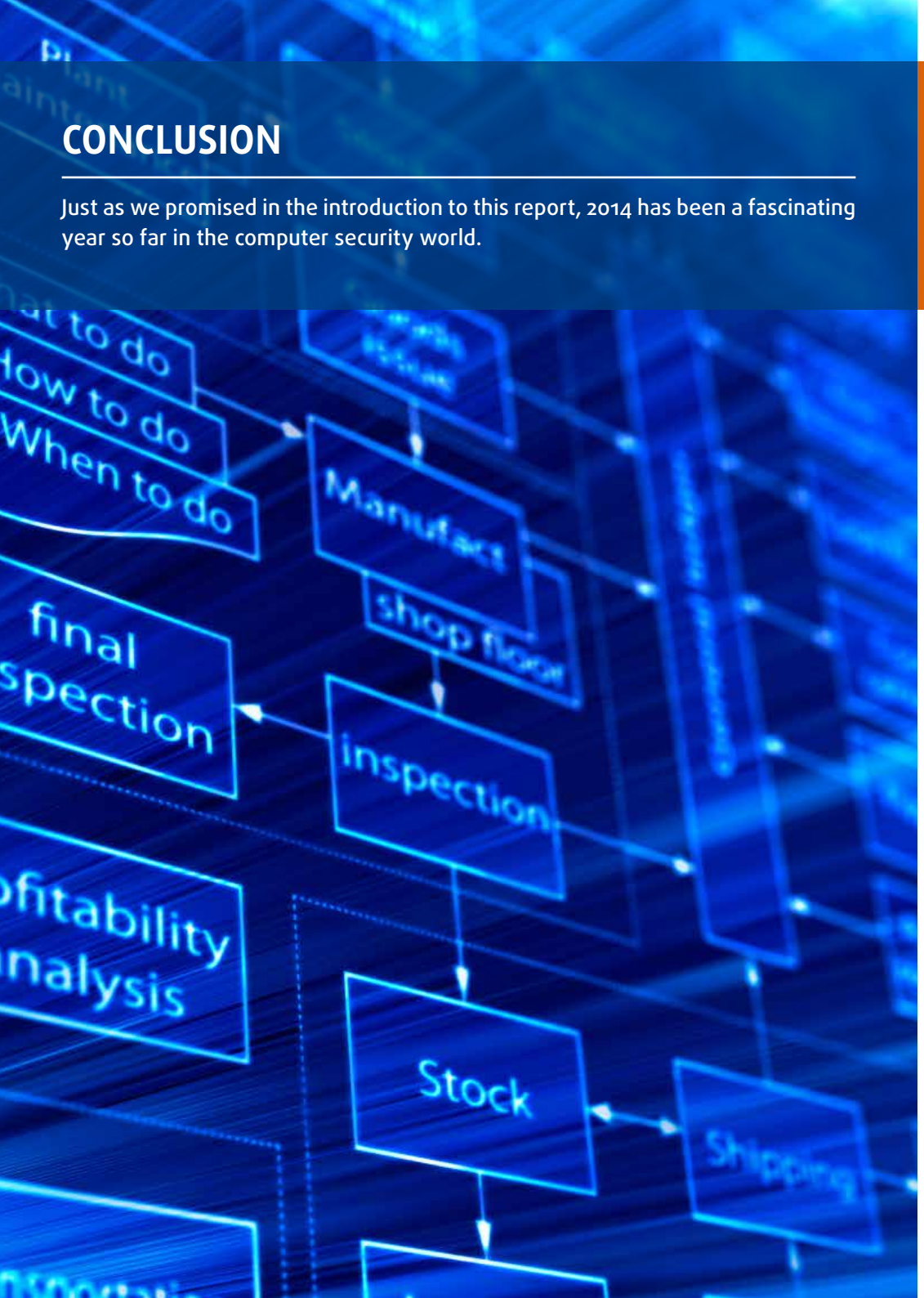
CYBER-WAR

In the cyber-war arena, new revelations continued to surface about the cyber-espionage activities carried out by the **NSA** and uncovered by Edward Snowden. New reports revealed the collaboration between the NSA and the British intelligence agency **GCHQ** (Government Communications Headquarters). One of the most controversial cases has to do to do with the "Optic Nerve" program, which accessed and collected webcam images from Yahoo users around the world. Although it's impossible to know the precise number of people that were spied on, it is estimated that in just six months, the webcams of more than 1.8 million users were hacked.

The NSA and GCHQ intercepted the webcam images of millions of Internet users through the "Optic Nerve" program

Instead of capturing whole video chats, the program randomly stored an image every five minutes. It is important to bear in mind that the victims were not suspected of any crimes. These were indiscriminate interceptions of individual users. It is also estimated that between three and eleven percent of the documents contained images of nudity. Yahoo accused British and U.S. intelligence of taking the violation of user privacy to a "whole new level."

In March, German newspaper Der Spiegel revealed how British intelligence agency GCHQ and US agency NSA had been spying on a number of German companies and individuals, including German Chancellor Angela Merkel.



CONCLUSION

Just as we promised in the introduction to this report, 2014 has been a fascinating year so far in the computer security world.

Malware creation hit record numbers, and companies worldwide have been the target of massive data thefts. Nevertheless, there has also been good news in the fight against cyber-crime, like the FBI's announcement that the mastermind behind SpyEye, one of the worst banking Trojans ever, pleaded guilty to bank fraud.

The attacks on Android devices continue to increase, affecting a growing number of devices. Our next reports will provide new details about these incidents, the most common security threats and the number of infections.

Meanwhile, visit the PandaLabs blog (http://www.pandalabs.com) to stay up to date with the latest discoveries made at the laboratory.

ABOUT PANDALABS

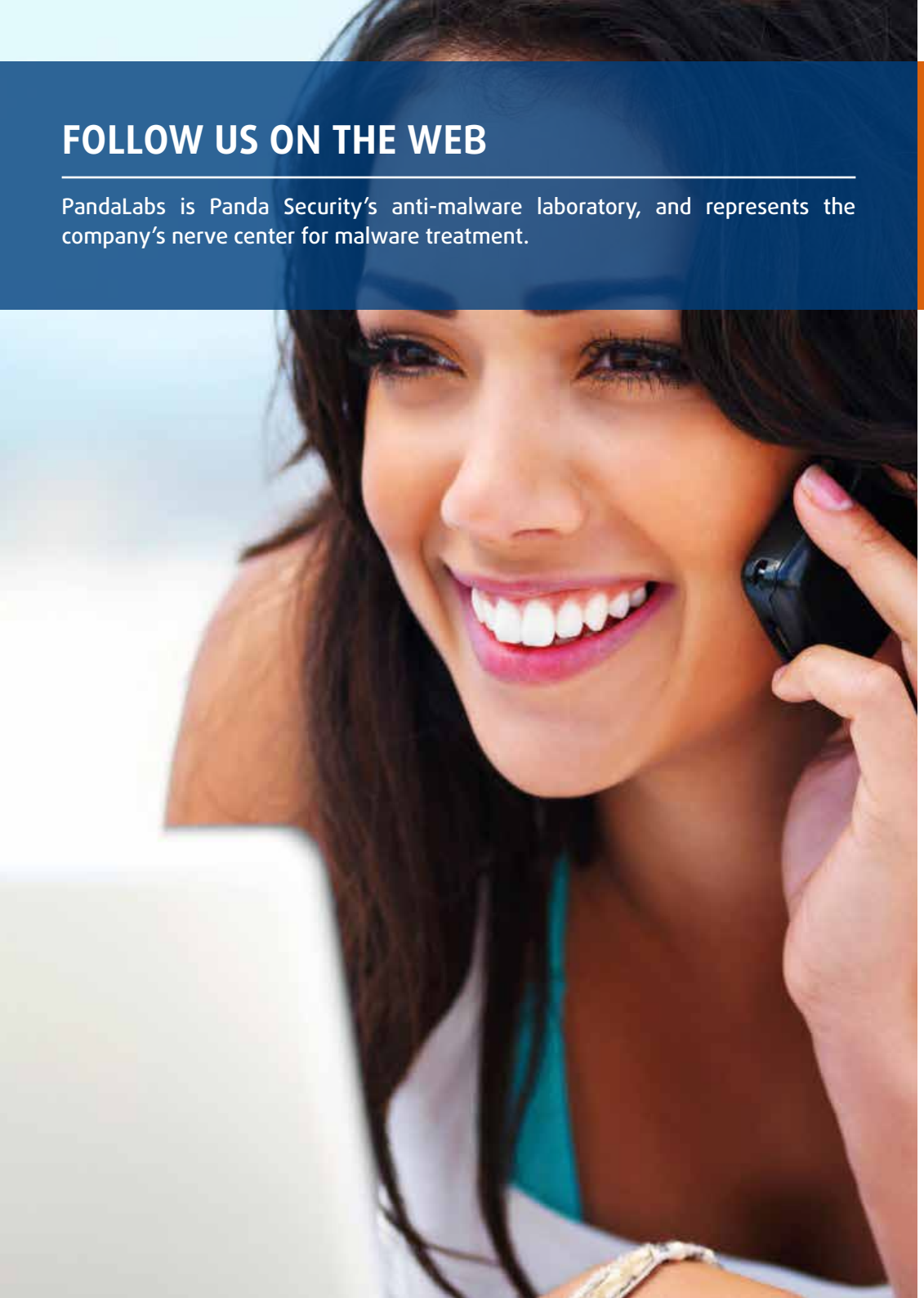
PandaLabs is Panda Security's anti-malware laboratory, and represents the company's nerve center for malware treatment.

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

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

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

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

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

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

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