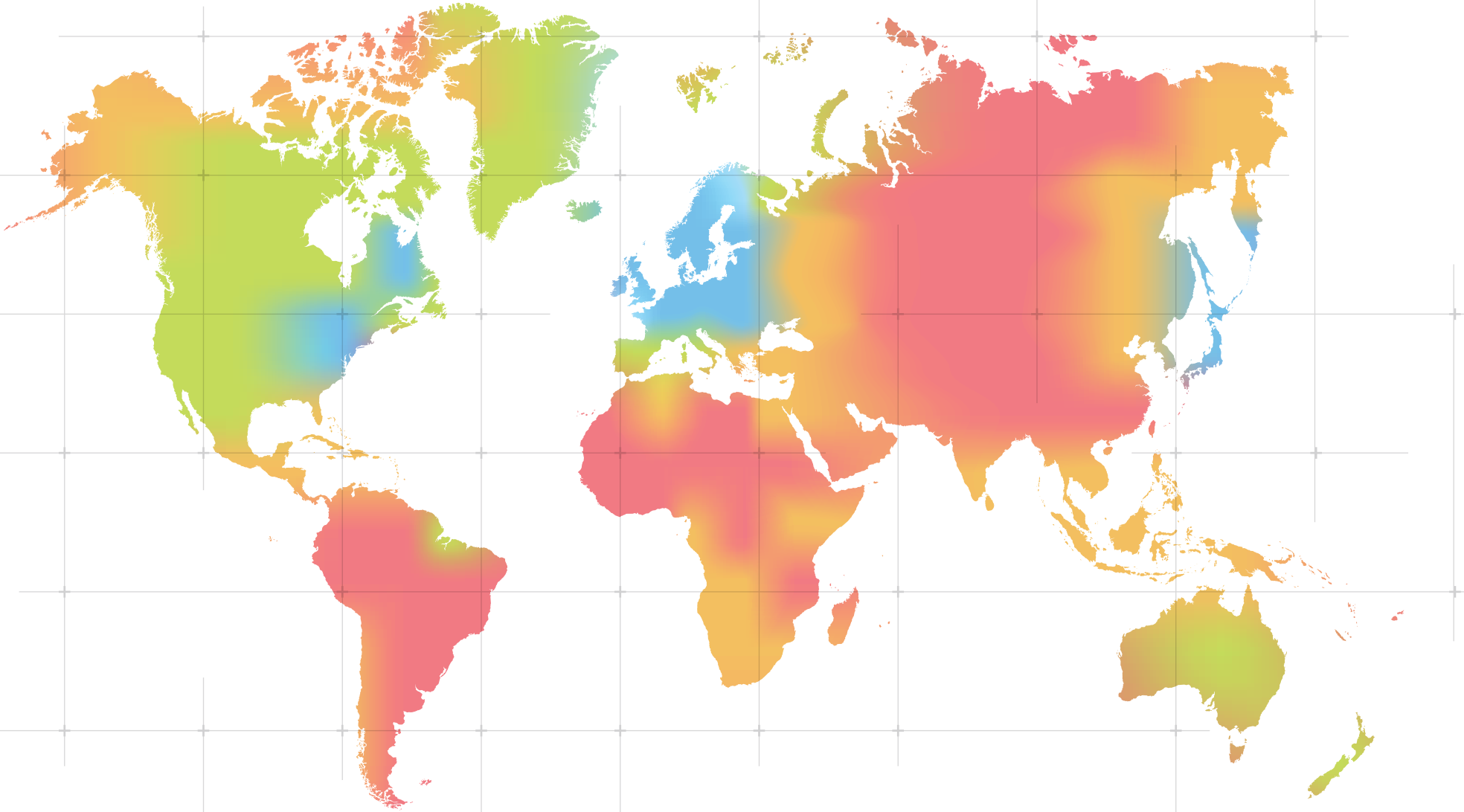
PANDALABS
THE EYE OF SECURITY



SPECIAL REPORT: 2015 FORECAST
AND THE MOST INFAMOUS ATTACKS OF 2014

PANDA SECURITY | *The Cloud Security Company*

SPECIAL REPORT: 2015 FORECAST

AND THE MOST INFAMOUS ATTACKS OF 2014

INTRODUCTION

According to estimates from PandaLabs, malware creation figures will once again break records in 2015.

Most of this malware will be designed for Windows platforms, though we will see a significant increase in threats targeting Android or Mac OSX.

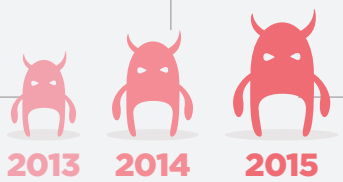
We can expect to witness an increase in Cryptlocker, malware which has already been prominent in 2014 and will continue to cause headaches in 2015.

Targeted attacks will also be more popular next year, and we will continue to see many Advanced Persistent Threats (APTs).

Mobile devices, particularly Android, will once again be in the sights of cyber-criminals.

Looking back at 2014, if anything stands out among all the events that took place it is surely the amount of attacks targeting major companies around the world, from leading technology giants like Dropbox, Paypal or Google to financial organizations, media companies and even celebrities.

In this PandaLabs report, we summarize the main IT security stories of the last year, and offer some security predictions to bear in mind to ensure you stay protected in 2015.



2015 SECURITY FORECAST

2013 was the year in which most malware ever was created. 2014 has beaten this record by a long way and it is set to continue growing in 2015 at a rate that will beat all of the records set to date.

The majority of this malware will be designed for Windows platforms but there will also be a significant increase in other types, such as Android and Mac OSX.

CRYPTOLOCKER

This type of malware has been in the spotlight in 2014, and these attacks are set to increase in 2015.

The functioning is quite straightforward: once it gets into a computer, it encrypts all types of documents that could be valuable to the user (spreadsheets, documents, databases, photos, etc.) and blackmails the victim into paying a ransom to recover the files.

Payment is always demanded in bitcoins, so that it cannot be traced by the police, making this type of attack very attractive to cyber-criminals, as many users decide to pay in order to recover the hijacked information.

TARGETED ATTACKS

Although the majority of malware attacks are within the millions of malware samples that appear every month, a small percentage of these are created to attack previously defined targets. These attacks known as targeted attacks are getting more common and will be very significant during 2015.

One of the greatest risks to tackle is that many companies do not think that they could be the target of targeted attacks, and therefore do not have appropriate measures for detecting them and stopping them, or at least for detecting any anomaly and mitigating any damage as soon as possible.

POINT-OF-SALE TERMINALS

During the year, attacks on POS terminals, used by all stores to take their customers' payment, have increased.

Cyber-criminals are effectively attacking these environments, allowing them to steal the credit card details of the customers of these stores. As a result, an activity that users did not think of as a risk, such as paying at a supermarket, gas station, clothes store, etc., is starting to pose a potential threat to which hundreds of millions of people around the world have already fallen victim.

APT

APTs (Advanced Persistent Threats) are a type of targeted attack aimed at companies or strategic institutions. Behind these attacks are usually countries that invest huge sums of money in ensuring that the target attack goes undetected for a long time.

They are the virtual version of James Bond. Although we will not see mass APT attacks in 2015, new cases will be discovered that will have probably been around for years but will only just start coming to light.

INTERNET OF THINGS

The number of Internet-enabled devices is increasing dramatically, and we are not just referring to computers or cell phones but other devices.

From IP cameras to printers, all of these "new" devices that form part of the Internet share a feature that makes them very vulnerable to becoming a target for cyber-criminals: they are devices that users do not pay much attention to and therefore, they are rarely updated, for example.

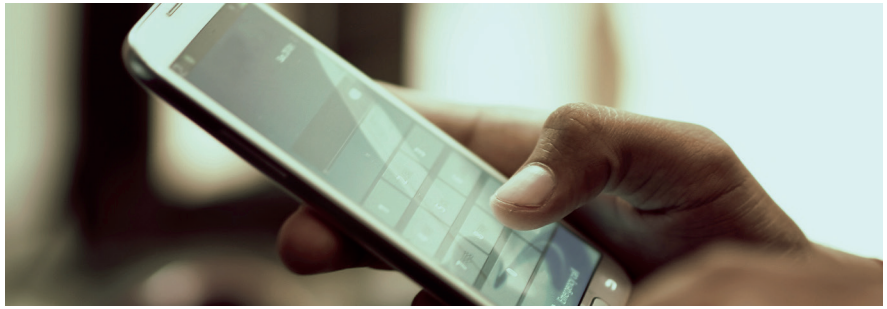
As a result, as soon as a security flaw is found in the software on any one of these, compromising the device will be child's play for any cyber-criminal.

To make matters even worse, these devices are connected to internal networks, home or corporate, making them ideal entry points for carrying out all types of wide-scale attacks.

SMARTPHONES

Smartphone attacks, or more specifically cell phones running Android, are going to reach new heights. Not only will the attacks increase but so will their complexity, with a single goal: to steal login details.

We store a growing amount of data on our smartphones and cyber-criminals are going to try to get it at any cost.



Although malware on cell phones was somewhat anecdotal a couple of years ago, more malware samples for Android have appeared in 2014 than all of the malware targeting any mobile device ever.

It seems that in 2015 growth will skyrocket, the number of victims also increasing, and therefore it will be essential to use antivirus products for these devices.

THE MOST INFAMOUS ATTACKS OF 2014

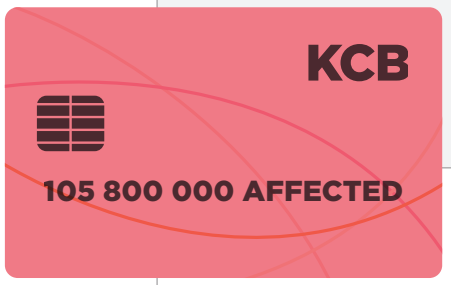
KCB

Credit firm Korea Credit Bureau (KCB) was the victim of an attack that stole the details of 105.8 million user accounts, including credit card details, first names and last names, telephone numbers, addresses and even passport numbers. The average Korean has five credit cards (the highest figure in the world), meaning that at least 21 million Korean citizens have had their details stolen. For a country with less than 50 million inhabitants, this suggests that at least 42% of the population has been affected by the attack.

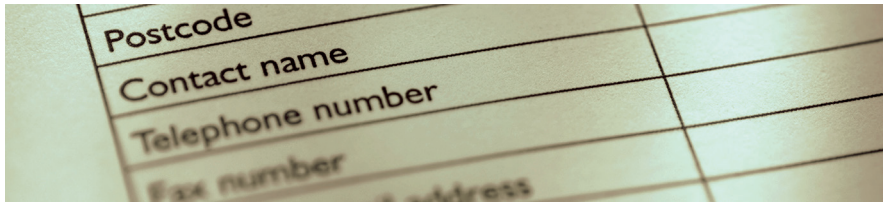
The real data however could be far higher, as not all victims will have had all their accounts stolen. With these types of numbers it would be easier to ask who in South Korea hasn't had their details stolen.

In this case there was no malware involved in the attack, rather the criminal worked for KBC –ironically in the company's anti-fraud team- and over eleven months compiled the information before selling it to the highest bidder. Had the data been adequately encrypted, the effects of the attack could have been mitigated, though this wasn't the case.

That anyone could steal information over a period of eleven months suggests there was a lack of supervision over access to the data processed by the firm.



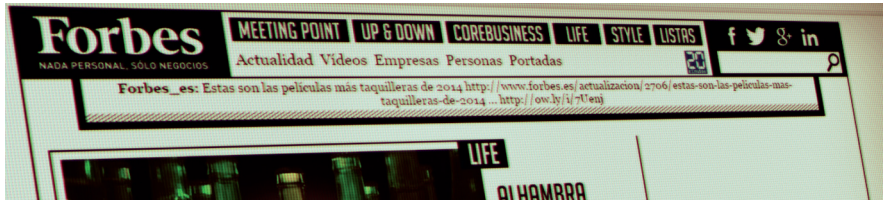
ORANGE



A vulnerability on the website of French telecom multinational Orange allowed attackers to obtain the data of thousands of customers, including their names, addresses and phone numbers.

Fortunately, it appears that Orange, despite the security hole, had sufficiently secured its systems so that passwords weren't compromised, thereby minimizing the damage to the 800,000 affected users. The passwords were apparently stored on another, more secure server.

FORBES



The Syrian Electronic Army (SEA) managed to compromise the Web page of Forbes, and stole data from more than a million users in the process, including hundreds of employees.

The information extracted included the names and email addresses of users, as well as encrypted passwords. Worse still, the SEA published the stolen data on the Internet.

EBAY AND PAYPAL, THE FIRST TO BE HIT

In May, eBay took us all by surprise when it asked users of PayPal, itsonline payment platform, to change their passwords.

The Internet auction site seemingly confirmed that cyber-criminals had accessed, a couple of months earlier, the accounts of some employees.

This, in turn, would have given them access to the company's internal network, and from there to the database with user names, phone numbers, email addresses and passwords.

They did assure however that neither the bank details nor the credit card data of customers had been compromised.

DOMINO'S PIZZA

Domino's Pizza was attacked by a group going by the name of 'Rex Mundi', stealing the data of 650,000 customers in France and Belgium. The group has demanded a ransom for the information, though the company has announced that it will not give in to blackmail.

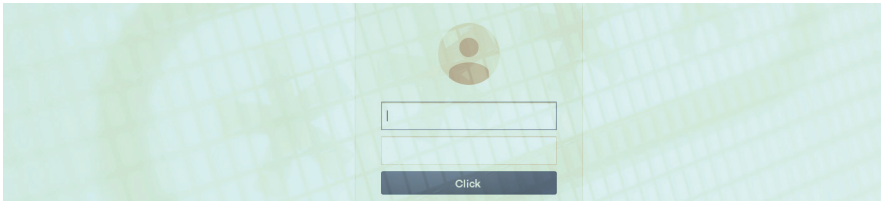
CELEBGATE: HOLLYWOOD IMAGES LEAKED TO THE WEB

September witnessed one of the most talked about attacks of 2014: CelebGate.

The leaking of nude images of 2013 Oscar winner, Jennifer Lawrence, as well as of other models and actresses via the 4Chan /b/ forum, was the subject of much debate. Apple claimed that the accounts of these celebrities "were compromised by a very targeted attack on user names, passwords and security questions". A practice "that has become all too common on the Internet".

This way, Apple denied that the hacking of these accounts was the result of a vulnerability in its iCloud or 'Find my iPhone' services.

THEFT OF FIVE MILLION GMAIL PASSWORDS



In September, a Russian cyber-security forum published a file with more than five million Gmail account details. Several experts confirmed that over 60% of the username/password combinations were valid. Google claimed however that the information was outdated, i.e. that the accounts either didn't exist or were no longer used.

Like Apple, it said there was no evidence that its systems had been compromised.

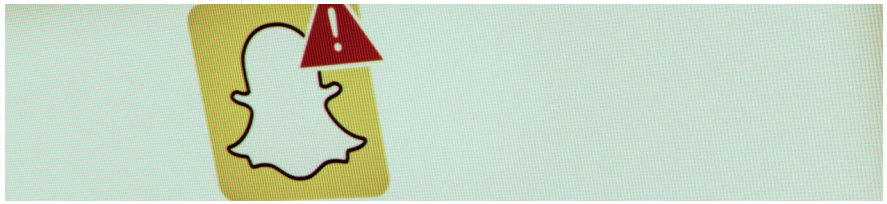
VIATOR AND USER BANK DETAILS

Also in September, Viator was the victim of a security attack through which cyber-criminals accessed the bank details of its users. Company sources said that the attack took place between September 2 and 3.

It appears that Viator became aware of the hacking thanks to complaints from customers about unauthorized charges on the credit cards used on the service.

As you would expect, and to prevent the theft of more data, Viator asked users tochange their account passwords and to keep an eye on any transactions charged against their credit cards.

SNAPCHAT



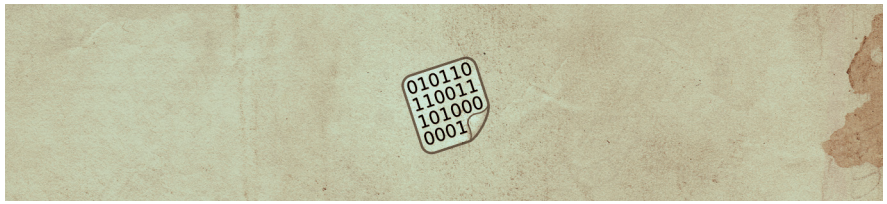
After the invasion of privacy of Hollywood actresses and models, in October, users of Snapchat had the security of their files compromised.

Snapchat is a mobile app for sending photos and images that are deleted between one and ten seconds after the message is read. Although Snapchat doesn't store users' images, another app, Snapsave, available for Android and iOS, does save them, and this enabled the theft of 200,000 photos.

HOME DEPOT

Home Depot, the DIY giant, acknowledged an IT attack on its servers that has compromised 56 million credit card details. According to The Wall Street Journal <http://online.wsj.com/articles/fraudulent-transactions-surface-in-wake-of-home-depot-breach-1411506081>, the company has also admitted that, in some cases, the accounts associated to the cards were emptied.

DROPBOX

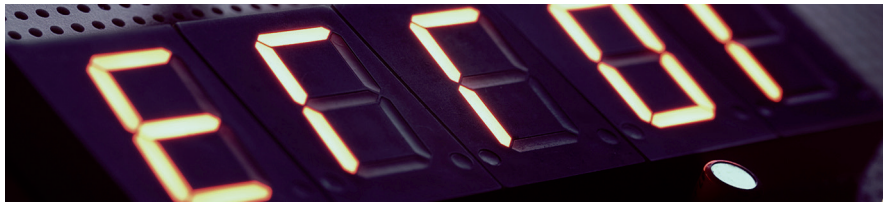


A user of Pastebin, a meeting point for hackers and IT security specialists, claimed to have obtained the passwords of seven million Dropbox users and, in order to prove this, made some of them public.

On the company's official blog, Dropbox was quick to announce that it had not been hacked, but that the data had been stolen from other services and consequently used to access its platform.

What does Dropbox advise? Not using the same password for all services and enabling two-step verification.

SONY



Towards the end of 2014 we saw one of the most serious targeted attacks against a company.

Many details are still unclear, though its effects have wreaked havoc on the Japanese company: an entire week without access to computers, massive destruction of data, theft of all types of internal company information... The attackers have publically posted five unreleased films and are threatening to continue publishing confidential information.

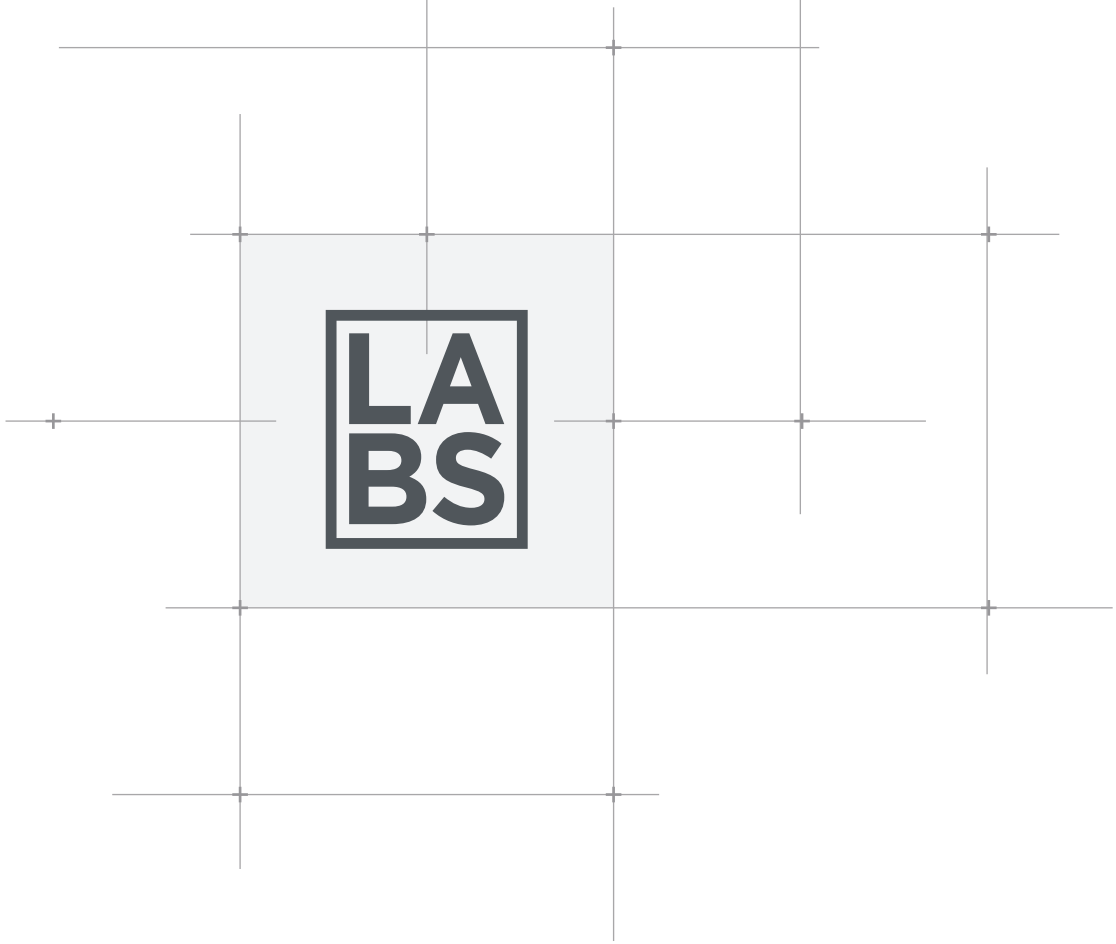
Malware has also begun to appear with Sony's digital signature, the credentials for which were stolen along with the rest of the information.

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.



facebook.com/PandaSecurity
twitter.com/Panda_Security
plus.google.com/+pandasecurity
youtube.com/PandaSecurity
linkedin.com/company/panda-security
www.pandasecurity.com/mediacenter/