ANNUAL REPORT
PandaLabs 2010

PANDA
SECURITY

We must admit that for those of us who have spent many years working in the world of security, 2010 has been particularly interesting. We have had everything: massive propagation of traditional, classic viruses; more BlackHat SEO attacks; social media used to distribute malware; hijacking of functions on popular websites, etc…

But overall, there is no doubt that 2010 has been a significant year in terms of security and privacy. Now, more than ever, we really feel that there is a genuine effort towards improving the security of businesses and individuals. Why? It's simple: several arrests have been made during the year (in particular, of course, those of Operation Mariposa), which were the result of investigative work by police forces in many countries. Even though there is a long way to go before we can feel truly secure, at least we are heading in the right direction.

It is also highly positive -in terms of awareness and education- that news related to security is seeing the light and the public are able to see what cyber-crime is all about. Some years ago, when we talked about cyber-war or cyber-terrorism, many journalists -people outside the world of security- looked at us as if we were talking about the latest Spielberg thriller. Now it is a reality (in fact it always was, but now it is reported).

Governments are taking it seriously, and are preparing themselves for what may happen. We will be looking at most significant stories to offer an insight into how serious this issue is. Cyber-security commands are being set up in several countries, along with improved legislation, preventive measures, etc.

This year has also witnessed the beginning of the era of cyber-protests or 'hacktivism'. The international coordination initiated by the Anonymous group in launching DDoS attacks against copyright protection societies, and later other organizations in support of Julian Assange, of Wikileaks, would appear to have stirred the virtual community into defending their rights and freedoms.

Apple's Mac also seems to have become a more popular target for cyber-criminals. Who, by the way, continue to profit enormously at the expense of innocent victim. This year more than 20 million new strains of malware have appeared, and we now have 60 million examples of malware classified in the Collective Intelligence database. Not an encouraging panorama… and certainly no time to drop your guard.

Microsoft has published 89 security updates this year, and Mac was already up to 175 by October. Android would also appear to be in the sights of cyber-criminals, although to a much lesser extent. So, once again there is more malware, designed with more ingenuity; with more distribution and infection vectors; exploiting numerous vulnerabilities; affecting more platforms… and… well why not just read this year's report? We hope you enjoy it!

This year has been an intense year for threats, and many issues have shaken the world of IT security. The dismantling of the Mariposa botnet, the "Here you Have" worm –an attack claimed by the Iraqi resistance-, 0-Day vulnerability exploits, Stuxnet and the attack on nuclear plants (SCADA systems), the Rainbow or OnMouseOver worm on Twitter, hijacking of the Facebook "Like" button, Android threats (such as FakePlayer), the launch of cyber-activism led by Anonymous, Wikileaks… In short, a year full of security-related events of all shapes and sizes. No doubt an indication that 2011 could be an interesting year.

Stuxnet, Iran and nuclear plants

This, without doubt, has been one of the incidents of the year. In July, we had news that a new worm, Stuxnet, had been discovered. Just one of the many thousands that appear every day, so why was this so special? At first glance it was a worm that spread through USB devices, like many others. But there was something special: simply by viewing the content of the USB drive, for example, using Windows Explorer, your computer would be infected. This was achieved through a 0-Day implemented in the worm, exploiting a previously unknown Windows vulnerability. As if this wasn't enough, it used other 0-Day vulnerabilities, as well as some that were already known.

To ensure that it went undetected, it installed a driver to implement rootkit techniques, a driver that was signed with legitimate -but stolen- digital signatures. Yet it didn't take any action on infected computers, other than self-propagating. Unless, that is, there was a Siemens PLC (Programmable Logic Controller) installed on the system. In this case it would use another unknown vulnerability, in the PLC, to read and write information.

So far all this is confirmed information, but this incident has also spurred a lot of rumors over the last few months. The complexity of Stuxnet suggests that it is the work of a team of highly specialized technicians, with considerable financial support (we're talking about millions of dollars), equipment and the ability to purchase 0-Day exploits on the black market. This has led to speculation that a country could be behind the attack. China? the USA? Nobody knows. But nevertheless, one vital ingredient was missing in this intriguing spy story: a target. Then a German researcher indicated that the infection ratio in

Iran was unusually high, and that these types of Siemens controllers were used in nuclear plants, such as the Bushehr plant in Iran. This led some to point the finger at Israel, particularly as there were references in Stuxnet that could be interpreted as the signature of the only democratic country in the Middle East.

FIG.01

NATANZ URANIUM ENRICHMENT CENTRIFUGE

In addition, there was another possible target of Stuxnet, the Natanz uranium enrichment centrifuge, which also use Siemens PLCs, meaning that Stuxnet could be used to alter the speed of the centrifuge equipment.

What we do know for sure is that the Bushehr nuclear plant was infected, or at least this has been **confirmed** by the Iranian authorities. In fact in December, the Iranian president **Mahmoud Ahmadinejad**, admitted that Stuxnet had affected the country's nuclear installations, confirming it as the outstanding incident of the year and one of the most spectacular in the history of cyber-crime or cyber-espionage.

Cyber-war

In addition to Stuxnet, there have been other incidents that have brought home the reality of cyber-war. In January, South Korea **announced** that it was setting up a special command center to combat potential cyber-attacks from North Korea and China. The United States also **acknowledged** the creation of the Navy Fleet Cyber Command, as a branch of the US military's cyber security force announced some months previously.

Along with these more serious incidences of what we could call cyber-war or perhaps cyber-defense, there have been some more 'colorful' incidents. Such was the case with the worm, dubbed 'Here you have'. This was the second variant of a worm that appeared in August, and one its main features is that the sender of the email message in which it spreads appears as "iraq_resistance", and would seem to be linked to the Brigades of Tariq bin Ziyad brigade terrorist group.

Three days after this variant appeared, someone claiming to be the author of the worm posted a video on Youtube, signed by 'IRAQ Resistance – Leader of Tarek Bin Ziad Group'. The poster used the alias "iqziad", and according to their YouTube profile is a 26-year-old living in Spain.

Tāriq ibn Ziyād al-Layti (Arabic, طارق بن زياد, (died in 720) was a Berber commander who led the Muslim invasion of the Iberian Peninsula in the eighth century, conquering Visigoth Hispania, according to traditionally accepted history, based on the Arab chronicles of the 10th and 11th centuries.

The video claims the worm has been created and propagated principally to target the United States for two reasons: to commemorate the 9/11 attacks and to demand respect for Islam, with reference to the threat made by pastor Terry Jones to burn the Koran.

The video displays a map of Andalusia, Spain along with a photo and an emblem, presumably that of the group. The video transcript is as follows:

"Hello, My nickname is Iraq Resistance. Listen to me about the reasons behind 9/September virus that affected NASA, Coca-Cola, Google, and most American ???. What I wanted to say is that the United States doesn't have the right to invade our people and steal the oil under the name of nuclear weapons. Have you seen any there? No evidence about any project. How easy you kill and destroy. Second, that the Christian, Terry Jones. What he tried to do the same day this worm spread is not even fair. I know that not all Christians are similar and some news papers wrote that I am a terrorist hacker because a computer virus and Mr. Terry Jones is not. And he is not terrorist because he affected all muslims behavior? I think, America, come on, be fair. Where is your freedom, which must end when you ???. As you say you modern educated people. I don't know that there is another one and really I don't like "smashing" and even there were no computers "smashed" as you know from the analysis report. I can "smash" all of those infected, but I wouldn't and don't use the word terrorist please. I hope all people understand that I'm not negative person. Thank you for publishing".

But going back to more serious events, we have seen how interest in these types of situations has become a reality, with governments in several countries understanding the need to be prepared for these kinds of attacks. The British prime minister, David Cameron, **announced** a fund of 650 million pounds for cyber-security. Concern is such, that in Europe a **series of trials** were launched simulating attacks on European institutions.

Aurora

We had barely entered 2010 when Google reported that a sophisticated and coordinated attack, dubbed 'Operation Aurora', had targeted a number of large multinational companies. Hackers had exploited a vulnerability in Internet Explorer to silently install a Trojan on computers, thereby remotely accessing users' confidential information.

This 0-Day vulnerability affected three versions of Internet Explorer (6, 7 and 8) on Windows 2000 SP4, WXP, 2003, Vista and Windows 7. The attack was called Aurora after investigators found the text string "aurora" in the source code of one of the Trojans involved in the attack. There are two theories about what hackers intended to achieve with this action: One argues that the intention was to steal intellectual property from large companies and the other, more simplistic, that the aim was to steal information from Gmail accounts of human rights activists in China.

Several Google employees in various countries received strange emails inviting them to access a Web page through a link. What happened then has been recognized as one of the most sophisticated cyber-attacks ever. The attack affected more than 30 multinational companies. Perhaps one of the most interesting aspects of this case, according to some sources, is that the people who received the emails were not chosen at random, rather they were high-ranking management who supposedly had privileged access rights to various applications. This is what we call a 'targeted attack', as opposed to massive or indiscriminate attacks.

The Trojan made encrypted connections to servers hosted in Texas and Taiwan. One of the main characteristics of the attack was the use of dynamic DNS, making it difficult to follow the trail. However, certain servers were identified which hosted domains registered by the Peng Yong 3322. org service in China, according to various technical reports. Google claimed that China was responsible for the attack, given that one of the source servers was in the country. The Chinese authorities denied all responsibility. It may well take some time before we really know the truth about Aurora. But as long as there are 0-Day vulnerabilities and users continue to fall for social engineering techniques, these attacks will continue to take place.

Cyber-crime

Despite all the talk about cyber-crime and cyber-espionage, we still can't afford to take our eye off profit-oriented cyber-crime, which continues to target businesses and individuals alike. In January, the FBI began to investigate the **theft of more than $3million** at a school in New York. In February it was discovered that more than $3 million had been stolen in a **phishing attack**. Incidents like these occur **every day**; they are not exceptional cases. Throughout the year we have seen numerous small companies **go under** thanks to these types of attacks, not to mention how unidentified groups, stealing small quantities from hundreds of thousands of users, have amounted as much as **$10 million**.

Criminals also profit by stealing information. One way of fighting against this is to combat the trafficking of information, no easy task, especially when it turns out that even governments are buying stolen data, **as was the case in Germany.**

Although the way to address the problem is to deal with those who are breaking law, that is easier said then done. It is easy to stereotype these criminals as young people, glued to their computers all day, but this is simply not true. The Internet is just a tool and can be used by any malicious individual. Take for example the US cyclist Floyd Landis, accused by a French court -who issued a warrant for his arrest- of having illegally hacked into the **French anti-doping agency's** computers.

One positive note this year is that it seems as though the Russian police have begun to take these crimes seriously, and we have seen the arrest of various Russian citizens accused of participating in these activities. Examples include the investigation into Igor Gusev or the arrest of 10 members of a **blackmail** gang.

Cyber-protests

Without doubt, in 2010 we have seen a turning point in the relation between Internet and society, with the emergence of the cyber-protest movement. This phenomenon, initiated by Anonymous, was not completely unheard of, but has become 'universal' in 2010.

Anonymous is a non-hierarchical group comprising thousands of users around the world, united in the defense of a common cause. Although the Anonymous group has been going for some years, they became more widely known when, along with The Pirate Bay, they supported the protests in Iran against the fraudulent elections in 2009 supposedly won by Mahmoud Ahmadinejad.

FIG.02

PAGE CREATED BY ANONYMOUS AND THE PIRATE BAY IN SUPPORT OF THE IRANIAN CITIZENS.

Yet it was in 2010 when the group really made the headlines. It all started when it came to light that several companies in the film industry had contracted the services of an Indian firm to launch denial of service attacks (DoS) against file-sharing websites that refused to remove certain links from their pages.

Anonymous was quick to organize an attack against the Indian company, although this was unsuccessful, and so it decided to target the film and music industry directly, along with anti-piracy associations. This worked in a similar way to 'real-world' protests, but taking advantage of the benefits offered by the Internet. Firstly, flyers were sent out (see below) looking for recruits:

FIG.03

ONLINE PROTEST AGAINST THE RIAA.

The action was a great success, and new targets were added; the same types of organizations but in different countries, such as the UK or Spain. After these attacks, we interviewed a member of the group to understand the motivation for the attack:

Q: Who is Anonymous?
A: I believe it is just a description of what we are. Anonymous is not an organization with hierarchy and leaders. We manifest as Anarchy. We are comprised of people from all walks of life. In short, we feel strongly motivated to do what we can to fight back against things which are morally questionable.

We fight back against the anti-piracy lobby. Pracy is the next step in a cultural revolution of shared information.

Q: What is your current mission?
A: To fight back against the anti-piracy lobby. There been a massive lobbyist-provoked surge in unfair infringements of personal freedom online, lately. See the Digital Economy Bill in the UK, and "three strikes" legislation in the EU which both threaten to disconnect internet connections based on accusations supplied by the music and movie industries. In the USA, a new bill has been proposed that could allow the USA to force top level registrars such as ICANN and Nominet to shut down websites, all with NO fair trial. Guilty until proven guilty! Our tactics are inspired by the very people who provoked us, AiPlex Software. A few weeks back they admitted to attacking file sharing sites with DDoS attacks.

We recommend reading our official statement here:
http://pastebin.com/kD52Af4N

Q: Do you advocate piracy?
A: Yes. It is the next step in a cultural revolution of shared information. Imagine it as the beginnings to an information singularity; a beginning of true "equality of opportunity", regardless of wealth or capacity. I would not have gotten anywhere near my accomplishments today without the books I pirated. I can't afford them!

Q: What websites have you attacked?
A: The Motion Picture Association of America [MPAA], The Recording Industry Association of America [RIAA], The British Phonographic Industry [BPI], The Australian Federation Against Copyright Theft [AFACT] ,Stichting Bescherming Rechten Entertainment Industrie Nederland [BREIN], ACS:Law, Aiplex, Websheriff, and Dglegal.

Q: Your original poster mentioned that "botnets" would be used in this attack. Do any of you profit from cyber crime?
A: That depends if you're using the anti-piracy lobby definition of cyber criminal or not. To be clear, we do not condone any sort of profit from botnets or malware for that matter, but the vast majority of what is constituted as Cyber Crime can be something as simple as downloading your favourite song, instead of paying ridiculous fees for that song (which the artist will only see a fraction of).

Q: What's your affiliation with 4chan? Are you all active members?
A: Some of us frequent 4chan, but we have no affiliation with any forum or website for that matter. We simply use them to communicate.

Q: How long will this attack go on for?
A: There is no time frame. We will keep going until we stop being angry

Q: Are you prepared to go to jail for your cause?
A: Yes, but we've taken every measure we can to make sure that our anonymity remains in tact. More importantly, why isn't this question asked to the very people who hired Aiplex to attack us in the first place?

Q: If you were able to resolve this situation, what would you want the respective media authorities of the world to do?
A: Personally, I would want them to basically go the fuck away altogether. Remove the barbaric laws they have lobbied for. Treat people like PEOPLE instead of criminals. Their long outdated traditional views on copyright infringement enforced solely by rich and powerful corporations need to be modified in light of the modern age on the Internet, the Information Age.

Artists under the media conglomerates have very little say in the content they produce and make a fraction of the profit. This is fairly evident with several mainstream artists who've now defected from the media regimes control. Take Nine Inch Nails and Radiohead as two great examples. Both groups have embraced piracy and have still continued to make a significant profit for themselves.

Q: Are you aware that this sort of attack is illegal in many countries and that your group can potentially put innocent people who support your cause under legal scrutiny?
A: I think that most people/participants are aware of that risk. In a world where our voice is ignored we feel we have no choice but to revert to direct action.

Q: Some people view this as the future of protests. Do you foresee future protests like this for other causes in the future?
A: Certainly. As for the protests, I hope the future of protests is ACTION. Not walking in circles with useless signs that are ignored.

Anonymous continued to act, but in December there was a change that dramatically increased its popularity. When Wikileaks started to receive attacks due to the pressure applied by the US government on various companies (suspension of Wikileaks' accounts from which they received donations through Paypal, Visa, Mastercard, canceling of the Amazon service hosting the website, etc.), Anonymous announced that it was supporting Wikileaks and would respond with DDoS attacks.

So started a series of attacks against the Web pages of PayPal, Mastercard, Visa, Postfinance, etc. Similarly, there were counterattacks (from unknown sources) against Anonymous. A 16-year-old was arrested in Holland, after which several attacks were launched against the websites of those responsible for the arrest (the police, courts, etc.). Days later, a 19-year-old was arrested in connection with these attacks.

FIG.04

TWITTER MESSAGE ANNOUNCING THE ATTACK ON MASTERCARD.COM

In some countries there is a legal void regarding taking part in DDoS (Distributed Denial of Service) attacks, but it is included in legislation in countries like Holland or the UK where sentences can stretch from two years (UK) to six years (Holland).

The media have referred to these incidents as 'cyber-war', which is inappropriate and far from the truth. They would be better classified as cyber-protests, and given their success during the second half of 2010, we are likely to see many more in 2011.

Mariposa

On March 3, 2010, at 10:00h, we announced… "*Panda Security and Defence Intelligence have co-ordinated the shutdown of a major botnet in collaboration with law enforcement agencies*".

According to the IT security companies Defence Intelligence and Panda Security, the Mariposa botnet, designed to steal confidential information, has been shut down by the authorities and is no longer in the control of the three suspected criminals accused of operating the botnet. The data stolen includes bank account and credit card details, user names and passwords from a global network of 12.7 million compromised computers belonging to home users, businesses, government agencies and universities from 190 countries. The botnet was dismantled in 2009 thanks to the combined efforts of security experts and law enforcement agencies, including Defence Intelligence, Panda Security, the FBI and the Spanish Civil guard.

With almost 13 million zombie computers, Mariposa is reckoned to be one of the largest botnets ever. Christopher Davis, CEO of Defence Intelligence, the first company to uncover the botnet, explained: "It would be easier for me to provide a list of the Fortune 1000 companies that weren't compromised, rather than the long list of those who were".

But this announcement was only possible after months of painstaking work… this is the story…

The making off
In May 2009, Defence Intelligence announced the discovery of a new botnet, dubbed "Mariposa". This discovery was followed by months of investigation, aimed at bringing down the criminal network behind what was to become one of the largest botnets on record.

Initial steps involved the creation of the Mariposa Working Group (MWG), comprising Defence Intelligence, the Georgia Tech Information Security Center and Panda Security, along with other international security experts and law enforcement agencies. The aim was to set up a task force to eradicate the botnet and bring the perpetrators to justice.

Once all the information had been compiled, the primary aim was to wrest control of the network from the cyber-criminals and identify them. Having located the control panels from which commands were sent to the network, we were able to see the types of activities the botnet was being used for.
These mainly involved rental of parts of the botnet to other criminals, theft of confidential credentials from infected computers, black-hat search engine optimization (on Google, etc.), and displaying pop-up ads.

The aim, in all cases, was clearly to profit from the botnet. The criminal gang behind Mariposa called themselves the DDP Team (Días de Pesadilla Team), as we discovered later when, due to a simple error, we were able to identify one of the alleged leaders of the gang.

Tracking down the criminals behind this operation had become extremely complex, as they always connected to the Mariposa control servers from anonymous VPN (Virtual Private Network) services, preventing us from identifying their real IP addresses.

On December 23, 2009, in a joint international operation, the Mariposa Working Group was able to take control of Mariposa. The gang's leader, alias Netkairo, seemingly rattled, tried at all costs to regain control of the botnet. As mentioned before, to connect to the Mariposa control servers the criminals used anonymous VPN services to cover their tracks, but on one occasion, when trying to gain control of the botnet, Netkairo made a fatal error: he connected directly from his home computer instead of using the VPN.

Netkairo finally regained control of Mariposa, and launched a denial of service attack against Defence Intelligence using all the bots in his control. This attack seriously impacted an ISP, leaving numerous clients without an Internet connection for several hours, including several Canadian universities and government institutions.

Once again, the Mariposa Working Group managed to prevent the DDP Team from accessing Mariposa. We changed the DNS configuration of the servers to which the bots connected, and at that moment we saw exactly how many bots were reporting. We we're shocked to find that more than 12 million IP addresses connecting and sending information to the control servers, making Mariposa one of the largest botnets in history.

On February 3, 2010, the Spanish Civil Guard arrested Netkairo. After the arrest of this 31-year-old Spaniard, police seized computer material that led to the capture of another two Spanish members of the gang: J.P.R., 30, a.k.a. "jonyloleante", and J.B.R., 25, a.k.a. "ostiator". Both of them were arrested on February 24, 2010. Victims of Mariposa include home users, companies, government agencies and universities in more than 190 countries.

Who was behind Mariposa?

Given the significance of the international operation, and the media interest generated, you might think it was the work of some of the greatest technical minds.

Yet analyzing their professional profiles, we reached the conclusion that, like many young people, computing is just a hobby for them and they are pretty much self-taught. It was probably by chance that they came across the idea –and knowledge required- to make such easy money.

And now...

Just when we had almost forgotten about Mariposa, this summer several arrests were made in Slovenia. People questioned whether this could really be related to Mariposa, as those behind Mariposa were Spanish and those arrested Slovene.

Last March, when the story was first announced, we talked about the Spaniards that had been apprehended, and that they had bought the bot. You may well remember that we said nothing about the seller of the bot. This wasn't because we didn't know who was behind it, but rather that the FBI had kindly asked us not to publish the information, as they were on the trail of Iserdo.

Who is Iserdo? It's the nickname of the Slovenian who developed the main Butterfly bot, and who was in contact with Netkairo. Similarly, he was the one who sold Netkairo the bot behind the Mariposa network.

According to Netkairo, he and Ostiator gave Iserdo "99%" of the idea to develop the bot. This is unlikely to be true; let's not forget that this 'revelation' was during a conversation in which Netkairo urged us to employ him in our laboratory.

After the arrests in Slovenia, the police gave a press conference revealing more information about the case. They searched seven addresses and confiscated some 75 devices (computers, hard drives, memories, etc.). They confirmed that two suspects, aged 23 and 24, had been arrested. After 48 hours both were released, but the investigation continues.

Police confirmed that one of those arrested is suspected of being the creator of the malware (known as ButterflyBot) with which the Mariposa botnet was created. They also indicated that they are investigating two crimes: the creation of tools facilitating digital crime and money laundering.

Let's hope that in our next Annual Report we also mention Mariposa, but that this time we are reporting the long sentences handed down to these cyber-criminals, in accordance with the crimes they have committed.

2010: The year of social media

It's not new, it's not surprising, and stories about the trend of exploiting social media for a range of criminal activities will no doubt fill the pages of our reports in 2011 and beyond… But this is a summary of what has happened in 2010, and the truth is there has much to talk about in terms of social media and security problems, and in particular related with privacy.

Basically, social networks have millions of users who every day, and for many hours a day, interconnect, interact, comment and even, sometimes, use them for work. And this is where the real danger lies: the number of potential victims among social media users has not escaped the attention of cyber-criminals. Let's start by taking a look at some figures…

First Annual Social Media Risk Index

Data from the **First Annual Social Media Risk Index** for SMBs shows the frequency with which social networks are used during work time (77% of employees admit to doing so), and consequently, 33% of companies have been infected by malware through this channel.

According to the study, the main concerns for SMB's with respect to social networks include privacy issues and financial loss (74%), malware infections (69%), loss of productivity (60%) and issues related with corporate reputation (50%), followed by network performance problems (29%).

Yet these concerns do not prevent SMBs from taking advantage of the benefits offered by social networks, with 78% of companies reporting that they use these tools to support research and competitive intelligence, improving customer services, implementing public relations and marketing initiatives and direct generation of revenue. Facebook is the most popular social media tool used by SMBs: 69% of companies have active accounts, followed by Twitter (44%), YouTube (32%) and LinkedIn (23%).

FIG.05
RESULTS OF THE USES
OF SOCIAL MEDIA TOOLS

Facebook, likewise, is mentioned as the main culprit in the case of malware infections (71.6%) and privacy violations (73.2%). YouTube is in second place in terms of infections (41.2%), while Twitter was responsible for a large number of privacy violations (51%). For those companies who reported financial loss through compromised employee privacy, Facebook was once again the social media from which most problems arose (62%), followed by Twitter (38%), YouTube (24%) and LinkedIn (11%).

**Millions of users = millions of potential victims**

In security terms, we've practically seen it all this year on social networks… One of the main aims of cyber-criminals has been identity theft: passing themselves off as friends or contacts of victims, hackers distribute content designed to trick users. This year's most popular technique for stealing identity works as follows:

Step 1: The bait

The bait normally comes from the profile of a friend whose account has already been hacked. Users typically receive a message (which appears to be genuine) suggesting the recipient clicks a link for one reason or another. In most cases, the message offers a "spectacular video" or claims "you appear in this clip", and normally includes the user name of the recipient.
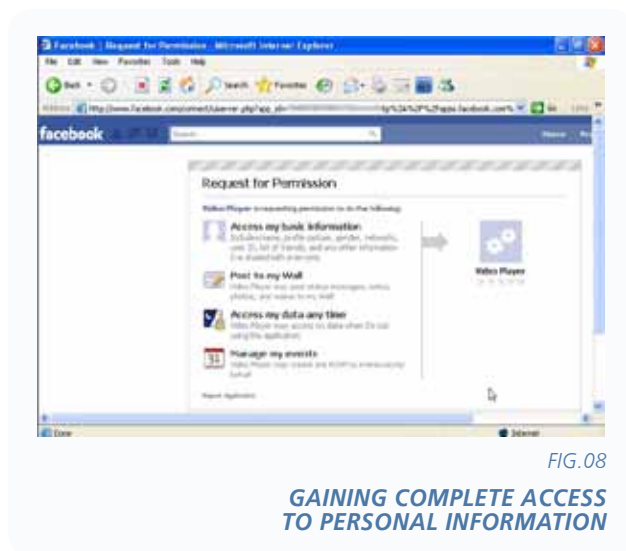
Example:

*MESSAGE OFFERS A "SPECTACULAR VIDEO"
OR CLAIMS "YOU APPEAR IN THIS CLIP*
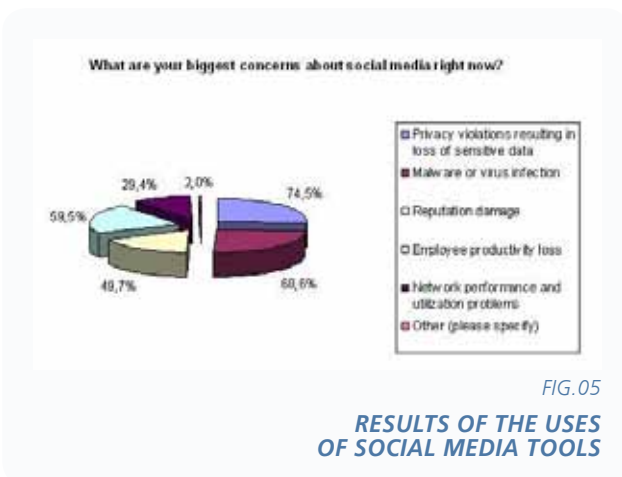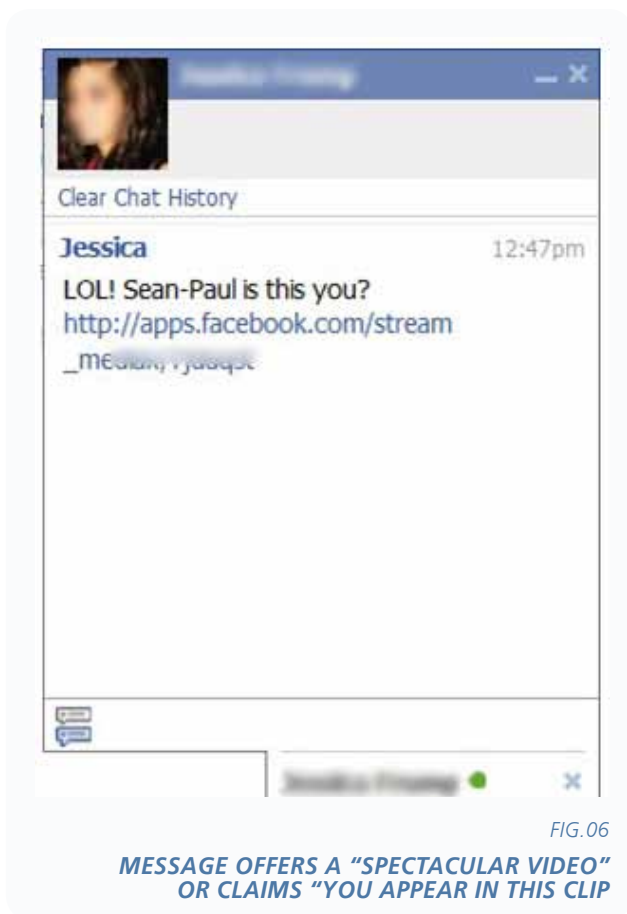
Step 2: Phishing attemp

Having attracted the attention of the user, cyber-crooks now need to get the user name and password of the intended victim to launch the second phase of the attack. The page that the link points to is a perfect replica of the Facebook login page, but is hosted on another Web address:

FIG.07

PHISHING ATTEMP
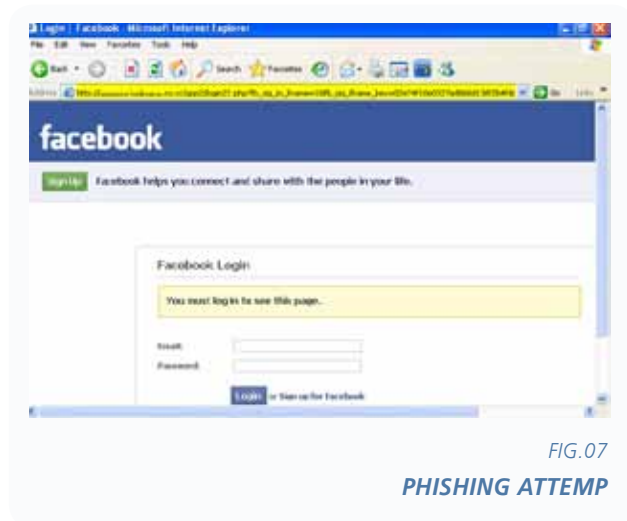
Step 3: Gaining complete access

Now the user has clicked the link and entered their login credentials, they have to grant the malicious application complete access to their personal information, as well as the rights to publish information through their profile. This ensures that the attack can be spread further through friends and contacts of the victim.

FIG.08

**GAINING COMPLETE ACCESS
TO PERSONAL INFORMATION**

After gaining the permission, the attack continues, targeting the victim's contacts and starting the process all over again with new users, as illustrated in the example below:

FIG.09

GAINING NEW USERS

Like it?

And speaking of Facebook, another technique widely used this year has been that of hijacking the "Like" button in the popular social network. Users could fall victim to this attack simply by accessing a Web page that contained Facebook's "Like" button, or through the social network's wall or internal messaging system, provided they were logged into the system. In this case, attackers try to attract users' attention by using subjects referring to games, movies, sex, etc. If the user clicks the malicious link, they are automatically redirected to a page with images and videos about the relevant topic. Once they access it, a reference to that page is immediately displayed in the user's profile together with the "Like" option and a text not controlled by the user.

This technique, known as 'clickjacking', uses a simple application to launch a javascript action. Visiting users are tricked into "liking" a page without necessarily realizing that they are recommending it to all of their Facebook friends. The real business stems from the pay-per-click system, which counts every visit and generates revenue for affiliates, and from the wide range of tests offered to users on these pages, which they have to pay for.

And speaking of hijacking and problems affecting security and privacy in social networks, back in May we uncovered a network for selling bots specialized in targeting social networking sites and free webmail systems. This publicly available Web page contained an extensive catalog of programs aimed at social networks and Webmail services like Twitter, Facebook, Hi5, MySpace, MyYearBook, YouTube, Tuenti, Gmail, Yahoo, etc.

FIG.10
SALES NET OF SPECIALIZED BOTS

Each of these bots was accompanied by a brief explanation of its purpose: creating a massive number of accounts on social networking sites; stealing identities, friends, followers or contacts; sending messages automatically, etc. According to the page: "All bots work in a conventional manner, they gather friend IDs/names and send friend requests, messages, comments automatically".

Prices ranged from $95 for the cheapest bot to $225 for the most expensive. The entire catalog could be bought for $4,500 and guaranteed that they would never be detected by any type of security solution, claiming that they had been developed to randomly change users, agents and headers as many times as is necessary to prevent them from being blocked. They also get round CAPTCHA security mechanisms included on many websites so that the buyer just has to set the parameters and leave the bots to operate on their own. Finally, the bots included perpetual updates.

Rogue antivirus solutions are everywhere…
At the beginning of the year we warned about the massive propagation of a false virus alert among Facebook users. The truth is, this was just another attempt to infect users with fake antivirus programs.

The fake warning was distributed via email and users forwarded it or published it on their walls, thereby spreading the hoax further. The text of the fake warning was as follows:

> ALERT — Has your facebook been running slow lately? Go to "Settings" and select "application settings", change the dropdown box to "added to profile". If you see one in there called "un named app" delete it… Its an internal spybot. Pass it on. about a minute ago….i checked and it was on mine.

There was no associated link but if users searched the Web for more information, they encountered numerous malicious websites designed to download fake antiviruses.
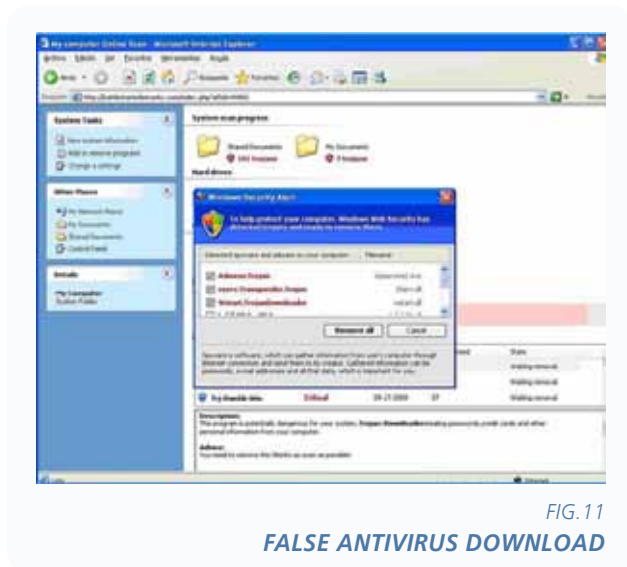

FIG.11
FALSE ANTIVIRUS DOWNLOAD

Yes, viruses for Mac also
This year we have seen how one of the most infamous Trojans targeting social networks –Koobface– reappeared and spread across the most popular sites once again. This time, however, it was specifically designed to attack Mac users. Using a video as bait, it tried to download some malicious Java codecs onto the user's computer. If the user agreed to the codec download, the malware installed on their computer and tried to download files from various servers.

This just shows what we have repeatedly said: As the Apple platform becomes more popular among users it is increasingly regarded by hackers as a good way to increase the number of victims of their attacks. This is just another example.

FIG.12
TROJANS ALSO FOR MAC

Going back to Koobface… It seemed that this year the Facebook security team was finally keeping the authors of this Trojan family at bay, who, according to estimates from the social networking site, were making the incredible amount of $35,000 every week (by tricking users, obviously). That makes 1.8 million dollars every year… Judging from this and other data in our hands, we can picture plenty of cyber-crooks repeating the title of one of my favorite Supertramp albums: "Crisis? What Crisis?".

Rogueware

2010 has without doubt been the year of the fake antivirus, and it's no surprise. There is a simple yet highly profitable business model behind this type of malware, and it is well worth the effort for criminals to spend a short while creating a new strain of rogueware and fake online store, safe in the knowledge that the victims will do their bit to provide the succulent returns.

Around 40% of all fake antivirus programs were created in 2010. Or in other words, since this new type of threat first appeared four years ago, at PandaLabs we have classified a total of 5,651,786 individual examples of fake antivirus programs, of these, 2,285,629 appeared between January and November 2010.

If we analyze all the examples classified of this type of threat with respect to all malware contained in our Collective Intelligence database (the automatic system we use to detect, analyze and classify 99.4% of the 63,000 new threats that appear every day), some 11.6% are fake antivirus programs. And let's not forget that this database contains all the malware detected in the 21 year history of our company, while rogueware only emerged four years ago.

Many users are still falling into this fraudulent trap thanks to the sophisticated designs, the authentic appearance of the messages and the powerful social engineering ploys used to convince victims that their computers are at risk. So far this year, 46.8% of computers around the world have been infected by some kind of malware: and 5.4% of them were infected with this type of program.

There are simply thousands of families of these threats and their variants, and the most widespread are as follows:
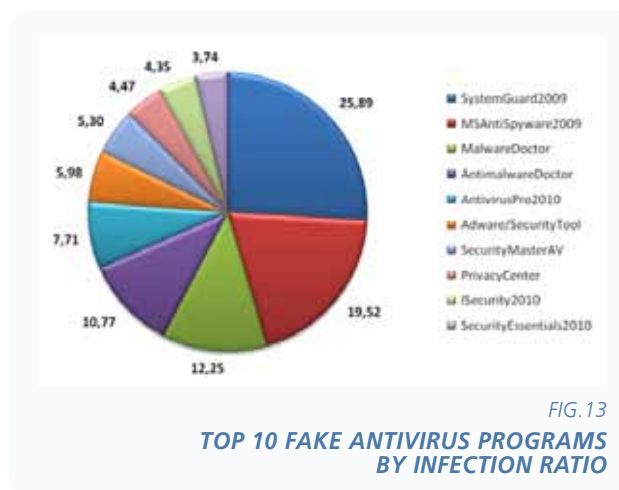

FIG.13
TOP 10 FAKE ANTIVIRUS PROGRAMS BY INFECTION RATIO

Every user that becomes a victim of a fake antivirus offers several benefits to hackers. Not only will they get the purchase price of the 'license' for the spoof program that will supposedly resolve all the problems –which of course is never received-, but they will also have the credit card details which can then be sold on the black market or used to withdraw cash, shop online, etc.

FIG.14
THE FAKE ANTIVIRUS THAT CAUSED MOST INFECTIONS IN 2010 WAS SYSTEMGUARD2009

According to the estimates put forward by PandaLabs in its paper **'The business of rogueware'**, the creators of these programs are raking in more than $34 million a month.

the use of SMS to defraud users. This is just another example of how hackers combine technologies and use all means at their disposal to make a profit.

As you may already know, most of these threats (if not all of them) come from Eastern European countries, including Russia and the Ukraine. However, this does not mean to say that cyber-criminals are deliberately trying to infect users from these regions. In fact many older examples of rogueware were programmed not to work if they detected a Russian keyboard. Although not anymore…

We have recently come across a rogueware site completely in Russian. It claims to offer protection for computers and social media profiles against spam, phishing, viruses and hackers.

This is what it looks like:

FIG.15
ROGUEWARE SITE COMPLETELY IN RUSSIAN

And this is the version translated into English (by Google translate):

FIG.16
TRANSLATED VERSION TO ENGLISH

After clicking the download button, several subscription options appear (all selected by default). Then a fake scan is run, after which you have to specify your country or region (Russia appears by default). Once you have selected one of the four cell phone providers indicated, a premium-rate number appears for sending an SMS along with the instructions for receiving the product activation code. The cost of the activation SMS is 300 rubles, around US$10.
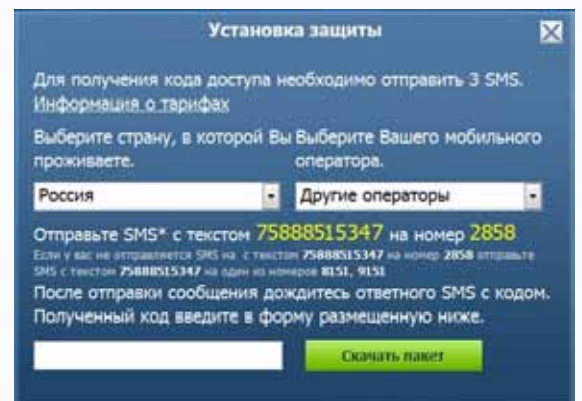

FIG.17
SMS IN RUSSIAN

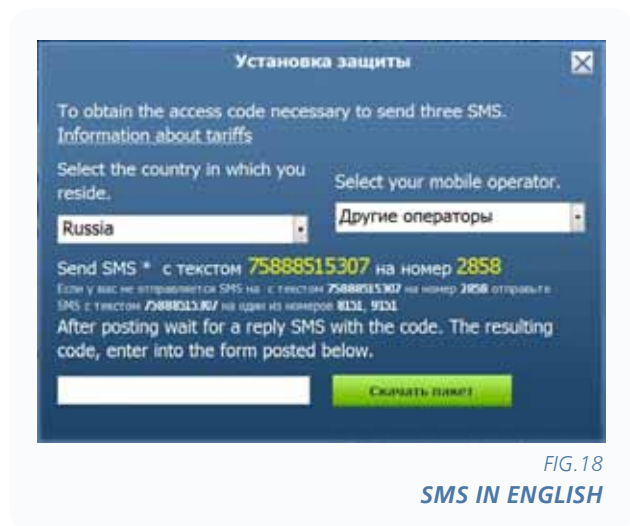And this is the version of the SMS translated into English (Google translate):

FIG.18
SMS IN ENGLISH

The story so far...

The fraudulent business of fake antivirus programs, otherwise known as rogueware, began in 2006, yet it wasn't until 2008 that these types of threats really began to spread. Users are normally infected after visiting certain websites and accepting downloads disguised as codec players or by clicking links in emails received, etc.

Once they have infected a computer, these applications pass themselves of as antivirus solutions, claiming to detect numerous threats on victims' systems. When users go to remove the threats with the fake program, they will be asked to buy the 'full' product license. Many users, concerned about the supposed infection of their system, end up buying the license. Once they have paid for the license, they will never hear from the vendor again, and the fake antivirus will remain on their computer.

FIG.19

THE PROFESSIONAL APPEARANCE OF THE FAKE ANTIVIRUS, WITH RECOGNIZED NAMES, HELPS LURE VICTIMS INTO PAYING FOR THE LICENSE

It is interesting to look back at previous annual reports, and compare how this section has begun over the years. Every year, we have collected and classified more malware than in previous years, and this has been the case since, in 2005, we first announced that cyber-criminals had become profit-oriented, and we consequently predicted a boom in malware circulation.

We would have loved to have been able to start off this section by telling you that there had been a drop in the amount of new malware, but nothing could be further from the truth. In 2010, have created and distributed **one third of all viruses that exist**. These means that **34% of all malware** ever created has appeared -and been classified by our company- in the last twelve months. What's more, Panda's Collective Intelligence database, which automatically detects, analyzes and classifies 99.4% of the threats received, now has **134 million separate files, 60 million of which are malware (viruses, worms, Trojans and other threats)**.

FIG.20
EVOLUTION OF NEW MALWARE CLASSIFIED BY PANDALABS
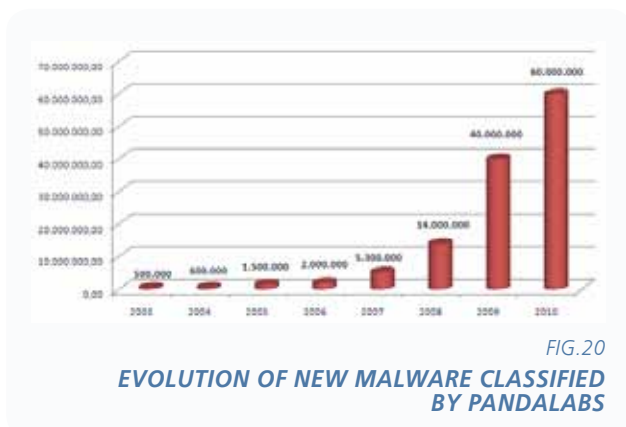
Rounding up the figures for 2010, some **20 million new strains** of malware have been created (including new threats and variants of existing families), the same amount as in the whole of 2009. The average number of new threats created **every day has risen from 55,000 to 63,000**.

The following figures give an idea of the sheer size of the data in our Collective Intelligence database:

The following figures give an idea of the sheer size of the data in our Collective Intelligence database:

• Some 113,000 new files are received every day by Collective Intelligence, of which 63,000 are new malware samples. 99.4% are processed automatically by Collective Intelligence in real time.

• 52% of the new malware processed by Collective Intelligence exists for just 24 hours.

• In 2010, Collective Intelligence processed more than 134,000,000 files, of which more than 20,000,000 were unknown or new malware.

• To do this manually would require 1,898 technicians and 3,705,388 hours of work.

• The Collective Intelligence database occupies more than 20,000 GB or 209 billion bits.

• If this amount of information were in text format, it would be equivalent to 808,192 volumes of the Encyclopedia Britannica, with almost 32 billion pages.

• Laid end-to-end, these printed pages would stretch for over nine million kilometers, the equivalent of going to the moon and back twelve times.

• And if we had to send this information across a standard ADSL connection, it would take 1,165 days.

This lets us confirm that the cyber-crime market is currently in rude health, although this is also possibly conditioned by the increasing number of cyber-crooks with limited technical knowledge who are turning their hand to these activities.

This also means that although more malicious software is created, its lifespan is shorter: 54% of examples are active for just 24 hours, as opposed to the lifespan of several months enjoyed by the threats of previous years. They now infect just a few systems and then disappear. As antiviruses become able to detect new malware, hackers modify them or create new ones so as to evade detection.

Despite these dramatic numbers, there is some good news, the speed with which the number of new threats is growing has dropped since 2009: since 2003, new threats grew by at least 100 percent every year. However, so far this year they have increased by around 50 percent.

As regards the **type of malware** created this year, there are no surprises: Trojans continue to dominate, although their relative share has dropped (from 66% last year to 55.9% this year) with a shift in favor of traditional viruses, which move up to second place in the ranking (from 6.6% in 2009 to 22% in 2010).

Adware, previously in second place (with 17%), has dropped to fourth place (9.6%). Worms meanwhile, are on the rise: from3% to 10%. Spyware has also dropped significantly: from 5.7% down to 0.34%.
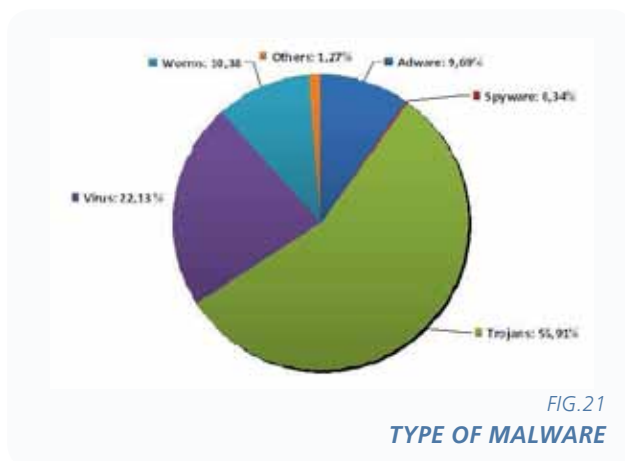
There is no surprise that Trojans remain as prevalent as ever, given that so many of them are designed for data or identity theft, information that can be sold on the black market. The rest, on the whole, continue to follow the trends observed over the last two years.

Some 1.26% of threats were in the category of 'others' which includes the usual suspects, distributed as follows:

Others	%
Dialer	29,11
Hacking Tool	26,91
PUP	24,28
Security Risk	19,17
Joke	0,48
Tracking Cookie	0,05

In terms of infections, we have calculated that an average of **53% of computer users** have been infected at some time by some type of malware, even with protection installed and up-to-date. This data has been gathered from users of the free, online solution **Panda ActiveScan 2.0**.

The Top 20 ranking of infections by country for 2010 is as follows:

FIG.21
TYPE OF MALWARE

FIG.22
TOP OF COUNTRIES WITH MORE INFECTIONS
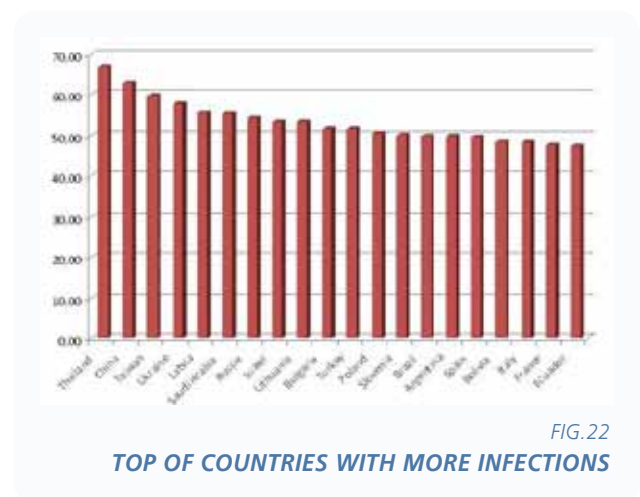
If we compare with the Top 20 ranking in 2009, there have been some significant changes. For example, Taiwan was top of the list but has now been overtaken by Thailand and China. Countries such as Poland, Colombia, Spain or Argentina have dropped right down the list or even disappeared. While others, like Italy or France, have seen their infection ratios drop. Sweden, Portugal and the UK have all disappeared from the ranking.

Regarding **infection methods**, 2010 has seen hackers exploit social media, the positioning of fake websites (BlackHat SEO techniques) and zero-day vulnerabilities.

BlackHat SEO is a maliciously-motivated search engine optimization technique that takes advantage of search engine functionality to promote malicious websites to the top of search results. BlackHat SEO perpetrators typically upload PHP scripts to hacked websites. These scripts query Google's trending topic service and then generate relevant HTML for the hottest search terms. The search engine is tricked into seeing the relevant material, but users are redirected to a malware distribution site when they click on the top search result link. Cyber criminals who leverage BlackHat SEO techniques to distribute malware are gaming search engines to the point where users may be put in a position where they can no longer trust search results – not good news for users or search engine companies. We have seen multiple BlackHat SEO campaigns targeting hot trending topics every single day this year, with many of them penetrating the top ranks of search results.

The first major BlackHat SEO campaign in 2010 targeted users searching for information on Google's Nexus One phone and on the earthquake in Haiti[1]. The first two search results for each pointed to rogueware campaign sites, and 5 out of the top 6 search results were malicious.

The next Blackhat SEO attack that got our attention targeted Facebook users[2]. This attack was different in that it did not exploit users via the typical Google trending topic method. Instead, the cyber criminals behind the attack chose to cross-pollinate their traditional Blackhat SEO campaigns with the timely announcement of a Facebook bug, which resulting in users seeing an "unnamed application" in their Facebook account settings. This was the first time we observed Blackhat SEO attempting to target social network users.

And the campaigns just kept on coming. There have been far too many to go into any significant detail on more of them, but some of the most notable attacks targeted holidays[3], sales events[4], natural disasters[5], much-anticipated product announcements[6], sporting events[7,8], celebrity gossip[9,10], TV shows[11], and popular toys[12]. The Blackhat SEO trend is likely to continue for as long as the Google trending topic service continues to be easily accessible to cyber criminals. Our research indicates that Google search results are the most vulnerable to Blackhat SEO, while Microsoft's Bing search results are relatively free of the scourge thus far.

[1] http://pandalabs.pandasecurity.com/blackhat-seo-attack-targeting-google-nexus-one/
[2] http://pandalabs.pandasecurity.com/unnamed-app/
[3] http://pandalabs.pandasecurity.com/malware-spreading-via-halloween-related-keywords/
[4] http://pandalabs.pandasecurity.com/blackhat-friday-and-cybercrime-monday/
[5] http://pandalabs.pandasecurity.com/out-of-the-frying-pan-into-the-fire/
[6] http://pandalabs.pandasecurity.com/this-time-it%e2%80%99s-apple-ipad%e2%80%99s-turn/
[7] http://pandalabs.pandasecurity.com/extreme-sports-2010-fifa-world-cup-bhseo-attack/
[8] http://pandalabs.pandasecurity.com/barcelona-vs-real-madrid-black-hat-seo-attack/
[9] http://pandalabs.pandasecurity.com/fernanda-romero-arrest-leads-to-distribution-of-rogueware/
[10] http://pandalabs.pandasecurity.com/chelsea-clinton-blackhat-seo-attack/
[11] http://pandalabs.pandasecurity.com/lost-ronnie-james-dio-and-so-on-and-so-forth-to-distribute-rogueware/
[12] http://pandalabs.pandasecurity.com/out-of-the-frying-pan-into-the-fire/

You can find many reviews on the Internet comparing Windows 7 and Mac OS X, analyzing which is faster, which has better effects and features, even contrasting the price, as the Apple system only costs $29.90. However, in this article we are going to look at the main security features offered by each one to tackle vulnerabilities and exploit techniques used nowadays to compromise systems.

Apple's market share is increasing, and as such, its operating system is now being targeted by malware developers. In fact, exploit kits that include this system are commonly available on the Internet, as is the case with "BackHole Kit Exploit", Russian software for creating botnets. In the following screenshot from this kit you can see the latest exploits for Apple, Mac OS X.

FIG.23
"BLACKHOLE KIT EXPLOIT", KIT OF MALWARE DISTRIBUTION THAT INCLUDES A MAC OS IN THE LIST OF VICTIMS
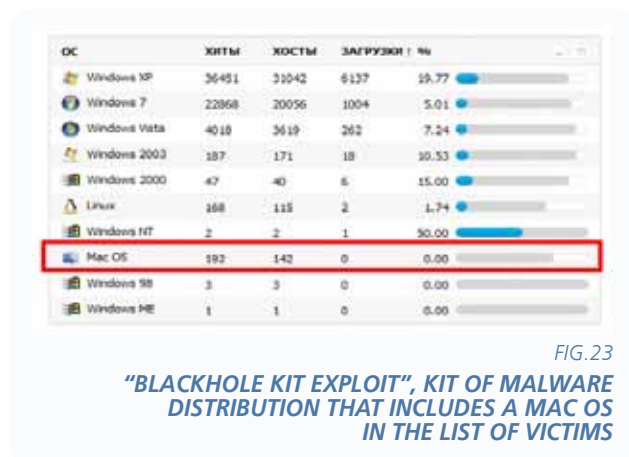
It is no surprise then that companies like Panda Security have launched security solutions[13] to combat threats that are now focusing on this platform.

Protection measures
Without going into too much technical detail we will now look at the two main security systems implemented in these platforms and the extent to which they make it difficult for hackers and cyber-criminals to exploit vulnerabilities and execute code on a vulnerable system.

DEP (Data Execution Prevention)[14]
This technique prevents the execution of data from a memory zone which does not have execution permissions. An attacker can use these zones to host malicious code before it is executed and if the DEP is enabled it prevents the code from being run, thereby protecting the system. DEP has been available on Microsoft systems since Windows XP Service Pack 2, however, Apple did not include DEP until the arrival of Snow Leopard, the latest available version of their system and the one we have used for this comparative review.

With respect to DEP, it's important to mention that there are two types of protection, one at the software level (Software-Enforced DEP also called SafeSEH) which prevents code from being run if, when an exception is thrown executing a program (which could be a vulnerability exploit), it tries to call an address outside the registered exception handlers. This system, although it prevents certain vulnerability exploits, does not constitute complete protection.

Hardware-Enforced DEP enables the NX /XD bit on compatible CPUs, and therefore depends on the hardware on which the operating system is running. This protection covers various possibilities for executing code from memory data zones. This protection can cause incompatibilities with legitimate software, and each program has to 'tell' the operating system whether or not it is compatible so that it can enable the protection when the process is launched. In other words, even though the operating system has the protection, if the software executed is not compatible with DEP, there will be no protection. Both Windows 7 and Snow Leopard have this protection enabled, for example, in Internet Explorer 8 and Safari.

13 http://prensa.pandasecurity.com/2010/10/panda-security-lanza-panda-antivirus-para-mac/
14 http://en.wikipedia.org/wiki/Data_Execution_Prevention
15 http://en.wikipedia.org/wiki/NX_bit
16 http://en.wikipedia.org/wiki/Address_space_layout_randomization

Although hardware-enforced DEP notably improves security, it is still less than adequate. There are certain attack techniques where a malicious user is able (depending on the version and configuration of Windows) to disable DEP in runtime for the program or simply grant execution permissions to the memory zone where the malicious code is stored before executing it. Either way, the DEP protection is evaded. To use either of these techniques, the malicious user must insert certain calls in the code to special operating system functions, and therefore the user must know the memory address of these functions. To avoid this, and prevent execution of malicious code, both operating systems implement ASLR (Address Space Layout Randomization) technology, available in Windows 7 and MacOS X since the Leopard version. Nevertheless, both in Leopard and in Snow Leopard it is less effective than the technology implemented by Microsoft in Windows 7. As mentioned previously, the application must be 100% compatible with ASLR for this mitigation technology to be effective.

ASLR modifies the memory address of the functions that the malicious user needs in every boot of the operating system so they will not know the location and the malicious code is not operative.

ASLR is effective provided that DEP is enabled and vice versa, otherwise a malicious user would be able to evade DEP or ASLR to execute malicious code. However, if both are enabled and the application is compatible with DEP and ASLR the chances of exploiting a vulnerability to execute malicious code are practically zero.

So after this brief analysis we can say that today, although both systems have adequate technology for tackling vulnerabilities, Microsoft Windows 7 is better prepared than Snow Leopard because its implementation of ASLR is superior to that of Apple. Mac OS X users will therefore have to wait to see how Apple responds with its new operating system, Mac OS X Lion.

In the various reports we have published this year, we have explained the process by which two platforms (iPhone and Android) have placed themselves as leaders in the smartphone market over competitors like Symbian and Windows Mobile. These two platforms have not been able to react fast enough to this new scenario and, despite releasing new versions of their operating systems in the last months of the year, don't seem to be the most popular options.

This new scenario has obviously affected the "malware market" by causing a reduction in the malware released for the Symbian and Windows Mobile platforms, which no longer look like an attractive prospect for hackers to invest in. Despite all this, there has still been a continuous, yet minor stream of malware for Symbian platforms, strongly focused on markets where they still have a strong presence, like Asia and emerging economies.

As for the platforms that are dominating the market, they have been mostly affected by phishing attempts through fake online banking services, proof-of-concept attacks and some spyware applications.

The future looks gloomy, and even though many consider Android the most vulnerable platform due to its application release policy, we have already explained in previous articles that this strategy could have precisely the contrary effect: Given that it is no longer necessary to root the phone, most users are turning to Android Market to download applications.

As already announced, the new Windows Mobile 7 is now available to users, and despite it not doing as well as expected sales wise, we should not underestimate Microsoft's sales force especially during the 2010-2011Christmas campaign, which will undoubtedly serve to boost sales and put the Redmond company's product among the leaders.

Let's see how the Android platform penetrates the market in 2011, as the number of cell phones with this operating system installed keeps growing and growing. It could also be the year when Internet connections through cell phones become commonplace, which may turn these platforms into a more attractive target for hackers.
Let's see what new strategies cyber-mafias put in place…
Whatever their tactics, we'll stay vigilant and always "One Step Ahead" to stop them.

Spam has continued at alarmingly high levels in 2010, although the dismantling of some botnets (such as Mariposa or Bredolad) has prevented these zombie computers from being used to send spam, with a consequent improvement in the situation. Last year, around 95% of all email traffic globally was spam, yet this figure dropped to an average of 85% in 2010.

Of all spam worldwide, some 50% is sent from just 20 countries, as illustrated below:

FIG.24
TOP 20 SENDERS OF SPAM IN 2010.
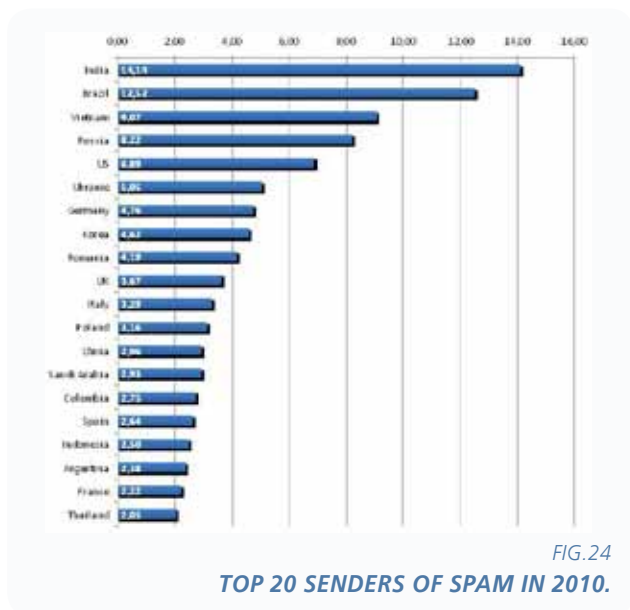
Pharmaceuticals continue to be the most popular subject of junk mail, followed by messages promoting fake designer products. Phishing messages designed to obtain online bank details and the like, as well as other fraud-oriented traffic have increased as a percentage of the total.

Yet this year we have seen some major new innovations in spam, which is no longer aimed solely at selling Viagra to the gullible using the most amateur-looking emails. We have witnessed spam campaigns exploiting new ruses designed to infect users.

Such was the case with an email designed to look like a message from the iTunes Store, perfectly imitating official communications from the store.

FIG.25
FALSE MESSAGE OF ITUNES.
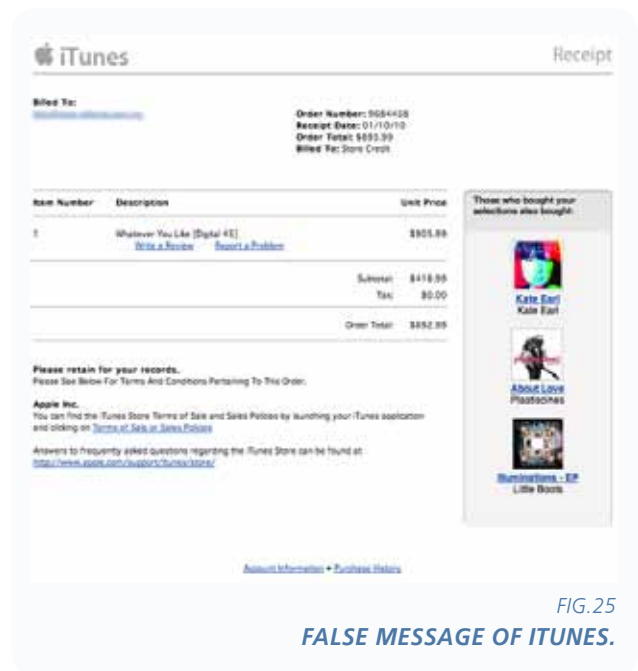
The real aim of this message is not to show products available on iTunes Store, but to entice users into clicking the "Report a problem" link which redirects to a fake Flash installer.

Another similar case has been detected involving the LinkedIn professional network. The message appears as if it has been sent from the address messages-noreply@bounce. linkedin.com on behalf of the LinkedIn communication department [communication@linkedin.com], and once again is a perfect copy of the LinkedIn email reminders.

FIG.26
MAIL MESSAGE SIMULATING LINKEDIN.

When the recipient goes to access the invitation, they are ultimately redirected to an online pharmaceutical store.

FIG.27
PHARMACEUTICAL STORE.

Social engineering techniques are still very much in vogue for tricking users, such as the 'Ministry of Transport' spam campaign, where a message -in very shaky English- advises recipients to read the attached documentation about vehicle license fee changes.

FIG.28
EXAMPLE OF SINOWAL.

Unsurprisingly, the documentation contained no information and was just an example of the notorious Sinowal virus.

Turning to zombies, PandaLabs has seen an average of 340,000 computers 'hijacked' every day. These computers, which form part of a botnet operated by cyber-criminals, are then used to send spam.

These services are offered, via the black market, at prices which are particularly attractive to vendors trying to sell products with no risk.

This service is not new, and is particularly aimed at users that want to send spam safely: databases with spammable addresses; rental of systems from which spam can be sent (botnets);   VPNs to connect anonymously to control panels, etc.

Here are just a few real examples of how these services are sold on the black market:

FIG.29
REAL EXAMPLES OF SALES SERVICES.

During 2010, excluding the publication of the December bulletin, Microsoft has published a total of 89 patches, affecting most of its products (Windows XP, Vista, 7, 2003 and 2008, Internet Explorer, MS IIS, MS Office, MS Exchange, MS SQLServer, Windows Media Player). There is no doubt that Microsoft continues to be the number one target for malware.

Of all these vulnerabilities, two design flaws in Microsoft Windows stand out. Around mid-June, a 0-Day vulnerability, CVE-2010-2568, appeared which affected all versions of Windows from Windows XP and even Beta versions of Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1 and was classified by Microsoft as critical.

The problem arises because Windows incorrectly handles shortcut files (.lnk and .pif), allowing a malicious user to execute remote code when a specially-crafted shortcut icon is viewed. The vulnerability was first exploited in the wild using the malware Rootkit/TmpHider. Because of the way it is exploited, as with the Autorun malware family, USB devices are the principal distribution vectors for malware that leverages this vulnerability.

As it was a critical vulnerability, Microsoft immediately published a workaround, though the solution was considered too 'aggressive', eliminating all Windows shortcut icons. The Internet community moved into action and other workarounds appeared, not connected to Microsoft, to mitigate the exploit of this vulnerability. Among them was the Ariad tool from the researcher Didier Stevens. Although there is now a patch for this vulnerability [MS10-046], it is not applicable in Windows XP SP2, and so tools like Ariad continue to be useful for protecting these versions of Windows that are outside the Microsoft security patch cycle. Some two months later, on August 2, Microsoft finally fixed the security hole with the publication -as mentioned- of MS10-046.

Adobe has also suffered a lot throughout the year, particularly with Adobe Acrobat and Adobe Reader. Attackers have concentrated their fire on these two products, as a simple way of infecting users. It is normal to be wary when you receive an email with an executable attachment, but not so much when you receive a PDF, and becoming infected by viewing a PDF online through your browser has horrendous implications.

Given the situation, many people opted to use Foxit Reader as a PDF reader, but all that glistens is not gold, and 0-Days have also appeared for this program. This serves to remind us that no program is 100% secure, there are just some programs that have yet to receive the full attention of malware developers.

One piece of good news is that Adobe has taken the initiative and published a new version of its PDF reader, Adobe Reader X, which includes a sandbox that adds an additional layer of security, so that even if the vulnerability is exploited, the environment in which the malware can operate is limited. It is effectively confined to the sandbox, restricting access to the system and preventing files from being overwritten or malware from being installed and run. This is a good initiative by Adobe. We will be keeping a close eye on how malware develops in this direction, as hackers will no doubt be looking for ways to bypass the sandbox.

We must also make mention in this section of the outstanding issue of the year: Stuxnet. This is one of the most complex examples of malware to emerge in recent years. Apart from being able to reprogram industrial PLCs (specifically Siemens WinCC SCADA systems), which means it can alter operational behavior in power plants, nuclear plants, etc. It also exploits five different vulnerabilities, four of them 0-days.

The vulnerabilities exploited are:

- • Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (MS08-067)
- • Microsoft Windows Shortcut 'LNK/PIF' Files Automatic File Execution Vulnerability (MS10-046)
- • Microsoft Windows Print Spooler Service Remote Code Execution Vulnerability (MS10-061)
- • Microsoft Windows Kernel-Mode Drivers Privilege Escalation (MS10-073)
- • Windows Task Scheduler Privilege Escalation

The first of these is an old issue, from 2008, but is still actively exploited by malware. MS10-046 was patched by Microsoft in August, with the MS10-046 bulletin, as we mentioned in the last couple, and the third vulnerability, MS10-061, was resolved in September. With respect to the last two, which allow privilege escalation, only the first has been resolved, with the publication in November of MS10-073. Microsoft has confirmed that the last of these will be patched in the near future, probably at the beginning of 2011, but no date has been set.

Pandalabs urges users to update all systems with the corresponding Microsoft patches, as MS10-046 and MS10-061 could allow remote execution of code, consequently permitting an attacker to take control of the system.

Over the last quarter, and to continue with vulnerabilities affecting Microsoft products, we would like to draw attention to a new vulnerability (CVE-2010-3962) affecting Internet Explorer 6, 7 and 8, allowing remote execution of code via CSS. Although in early November, this vulnerability was barely being used by malware, this is no longer the case by the middle of the month, with the publication of exploits, and so no doubt Microsoft will shortly release a patch.

Mozilla Firefox was also impacted by a 0-Day that appeared around the beginning of October, affecting versions 3.5 and 3.6 of the browser. Among other consequences, the Nobel Prize website was compromised by having the code needed to exploit this vulnerability injected. At the end of October, Firefox published updates for Firefox and Thunderbird to resolve the problem.

Going back to Adobe, in this last quarter we have once again seen 0-Day exploits for their products. At the end of October, a new 0-Day affected various versions of Adobe Flash Player, specifically 10.1.85.3 in Windows, Macintosh, Linux and Solaris, 10.1.95.2 in Android, the authplay.dll component of Adobe Reader 9.4 for Windows, Macintosh and UNIX and Adobe Acrobat 9.4 for Windows and Macintosh. This vulnerability, identified as CVE-2010-3654, allows remote execution of code. It was a 0-day actively exploited by malware, leading Adobe to publish the corresponding solutions.

There will be few radical innovations in cyber-crime during 2011. **Cyber activism** and **cyber war**; **more malware** aimed at generating a profit, **social media**, **social engineering** and **malicious codes with the ability to adapt** to avoid detection will be the main protagonists in 2011. There will also be an increase in the **threats to Mac users**, new efforts to attack **64-bit systems** and new **zero-day exploits**.

Once again we have dusted off the crystal ball and this is a summary of what we reckon will be the ten major security trends during 2011:

1. Malware creation. In 2010 we have seen a significant growth in the amount of malware, which has been a constant theme of the last few years. This year, more than 20 million new strains have been created, more than in 2009. At present, Panda's Collective Intelligence database stores a total of over 60 million classified threats. The actual rate of growth year-on-year however, appears to have peaked: Some years ago it was over 100%. In 2010 it was 50%. We will have to wait and see what happens in 2011.

2. Cyber war. Stuxnet and the Wikileaks cables suggesting the involvement of the Chinese government in the cyber-attacks on Google and other targets have marked a turning point in the history of these conflicts. In cyber wars, as with other real-world conflicts today, there are no ranks of uniformed troops making it easy to distinguish between one side and another. This is like guerrilla warfare, where it is impossible to discern who is launching the attack or from where. The only thing it is possible to ascertain is the objective.

In the case of Stuxnet, it was clearly an attempt to interfere with processes in nuclear plants, Specifically, with uranium centrifuge. Attacks such as these, albeit more or less sophisticated, are still ongoing, and will no doubt increase during 2011, although many of them will go unnoticed by the general public.

3. Cyber-protests. Undoubtedly the major new issue in 2010. Cyber-protests -or hacktivism- are all the rage. This new movement was initiated by the Anonymous group and Operation Payback, targeting firstly organizations trying to close the net on Internet piracy, and later in support of Julian Assange, founder of Wikileaks. Even

users with limited technical know-how can join in the distributed denial of service attacks (DDoS) or spam campaigns.

Despite hasty attempts in many countries to pass legislation to counter this type of activity, effectively by criminalizing it, we believe that in 2011 there will be yet more cyber-protests, organized by this group or others that will begin to emerge. The Internet is increasingly important in our lives and is a channel for expression that offers anonymity and freedom, at least at the moment, so we will no doubt see more examples of this kind of civil protest.

4. Social engineering. There is a saying that goes something like "humans are the only animals to trip twice over the same stone". Surely this is true, and one good example of this is the continued use of social engineering to infect unwary users. In particular, cyber-criminals have found social media sites to be their perfect working environment, as users are even more trusting than with other types of tools, such as email.

Throughout 2010 we have witnessed various attacks that have used the two most popular social networks - Facebook and Twitter- as a launch pad. In 2011 we fully expect that not only will hackers continue to use these media, but that they will also be used more for distributed attacks.

Moreover, BlackHat SEO attacks (indexing and positioning of fake websites in search engines) will also be widely employed throughout 2011, as always, taking advantage of hot topics to reach as many users as possible.

With the continued expansion of all types of multimedia content (photos, videos, etc.), a significant amount of malware will be disguised as plugins, media players and other similar applications. It is not so much that other methods have disappeared, such as PowerPoint presentations passed on from friend to friend, but security education and awareness campaigns have taught users to be wary of these types of applications.

As ingenuity often flourishes in times of crisis, and sadly, as technical expertise is increasingly less necessary for cyber-criminals, we are bound to see waves of new and convincing methods designed to trick unwary users: romantic offers online, spoof job adverts, increasingly

sophisticated scams, phishing attacks not just targeting banks but also pay platforms, online stores, etc…

In short, now more than ever, common sense is one of the most important defensive tools for securing our online lives, though as is often said, this is the least common of the senses.

5. Windows 7 influencing malware development.
As we mentioned last year, it will take at least two years before we start to see the proliferation of threats designed specifically for Windows 7. In 2010 we have begun to see a shift in this direction, and we imagine that in 2011 we will continue to see new cases of malware targeting users of this new operating system.

6. Cell phones. The eternal question: When will malware for cell phones really take off? It would seem that in 2011 there will be new attacks, but still not on a massive scale. Most of the existing threats target devices with Symbian, an operating system which is now on the wane. Of the emerging systems, PandaLabs' crystal ball tells us that the number of threats for Android will increase considerably throughout the year, becoming the number one target for cyber-crooks.

7. Tablets? The overwhelming dominance of iPad in this terrain will start to be challenged by new competitors entering the market. Nevertheless, save the odd proof-of-concept or experimental attack, we don't believe that tablet PCs will become a major consideration for the criminal fraternity in 2007.

8. Mac. Malware for Mac exists, and will continue to exist. And as the market share continues to grow, so the number of threats will grow accordingly. Of most concern is the number of security holes affecting the Apple operating system. Let's hope they get 'patching' as soon as possible, as hackers are well aware of the possibilities that such vulnerabilities offer for propagating malware.

9. HTML5. What could come to replace Flash, HTML5, is the perfect target for many types of criminals. The fact it can be run by browsers without any plug-ins makes it even more attractive to find a security hole that can be exploited to attack users regardless of which browser they use. We will see the first attacks in the coming months.

10. Highly dynamic and encrypted threats.
This is something we have already seen over the last two years, and we fully expect this to increase in 2011. There is nothing new about profit-motivated malware, the use of social engineering or silent threats designed to operate without victims realizing. Yet in our anti-malware laboratory we are receiving more and more encrypted, stealth threats designed to connect to a server and update themselves before security companies can detect them. There are also more threats that target specific users, particularly companies, as information stolen from businesses will fetch a higher price on the black market.

The overall picture is not improving. It is true that in 2010 we have seen several major arrests that have hit hard in the world of cyber-crime. Yet this is sadly insufficient when we consider the scale of what we are fighting against. Profits from this black market amount to thousands of millions of dollars, and many criminals operate with impunity thanks to the anonymity of the Internet and numerous legal loopholes. The economic climate has contributed to the seriousness of the situation: as unemployment grows in numerous countries, many people see this as a low risk opportunity to earn money, though this does not detract from the fact that it is a crime.

PANDA SECURITY

When we tell people about everything that is happening and we see their reaction, we usually ask them what they think about the situation… We will not repeat the answer we normally get (it might be a bit too crude and colloquial), so let's just say that it scares them.

It is true that from a global perspective, the situation looks serious. And rightfully so. However, this shouldn't discourage us from using the Internet, online banking or shopping services, social networking sites… That is, it shouldn't prevent us from enjoying everything good the Internet has to offer.

It only means that we must be wary, cautious and ready for anything that may happen. Unfortunately, the real world also suffers from insecurity (maybe now even more due to the financial crisis), and that doesn't prevent us from going out and living a normal life. However, we must stay alert and avoid running unnecessary risks.

We are sure that the 2011 year will be much more interesting with regards to malware, and maybe more dangerous too. However, our will to keep defending security both in the public and private arena will bring us forward in our struggle to defeat this most tenacious enemy.

We hope you have a good start to the New Year and achieve all you expect in 2011… in the security field as well. Happy 2011!

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/*