



ANNUAL REPORT

PandaLabs 2009

© Panda Security 2009

PANDA | 20th Anniversary
SECURITY 1990-2010

Introduction	03
2009 in figures	04
Global consequences of malware	05
2009 – The year at a glance	06
The harsh reality	06
It's not all bad news	07
Social engineering, social networks and Web 2.0	07
Cyber war: myth or reality?	10
Threats in 2009	12
The profitability of rogueware	12
Banker Trojans	14
2009: The year of Conficker	14
Spam in 2009	16
Main vulnerabilities in 2009	19
Trends in 2010	20
About Pandalabs	22

The last 12 months really have marked a turning point in the history of IT security. This has been for several reasons, yet without doubt the main one has been the way in which criminal organizations have consolidated underground business models. In 2009, hackers have made more money than in any previous year, underlined not least by the total number of new and different malware samples received by PandaLabs throughout the year, exceeding by far the forecasts we made in 2008. At time of writing, there are over 40 million malware samples in our Collective Intelligence system, and we are still receiving an average of 55,000 new samples every day.

This trend, which began in 2008 and has been consolidated in 2009, will continue to determine the day-to-day activity of anti-malware laboratories during 2010.

In 2009, banker Trojans and fake antiviruses have captured the media's attention more than any other threats, although viruses, which have made an unwelcome resurgence (Conficker, Sality and Virutas), also deserve a mention.

As for distribution methods, social networks have made the headlines in 2009, providing new alternatives for the propagation of malware. Additionally, cyber-crooks have professionalized SEO techniques to promote malicious websites (from which malware is distributed) through the most popular search engines, such as Google, exploiting the most topical issues of the day (Michael Jackson's death, popular events, etc.).

If we also consider the exponential growth of malware and the new distribution channels available to cyber-criminals, it is evident that the need for good protection is as strong as ever, but that it is also essential to invest in training and education for users, who are still the weakest link in the security chain.

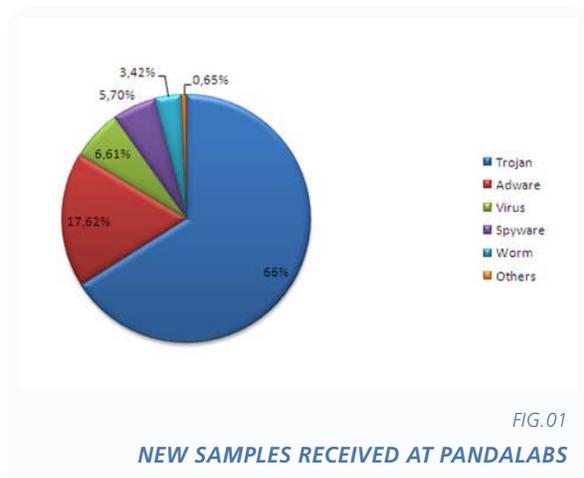
Curiously, just as President Obama has acknowledged the potential threat from cyber-crime to individuals as well as to critical national infrastructures, we are witnessing increased media coverage of cyber-war and cyber-terrorism. Scenarios that were once the terrain of sci-fi movies are now becoming a reality.

In this report we will take a look at how malware is evolving worldwide and we will try to analyze the main trends of 2010. Without revealing too much, let's just say the future doesn't look too bright.

The year 2009, in which Panda Security is celebrating its 20th anniversary, has seen the company detect more new malware than in any other year throughout its history.

The current boom in cyber-crime and Internet mafias is fueled by the positive results they are enjoying. Criminal business models and the affiliation networks used to increase profitability have been consolidated, while new malware creation and distribution techniques are emerging continuously.

In 2009, the total number of individual malware samples in Panda's database reached 40 million, and we believe this will continue to increase throughout 2010. We receive 55,000 daily samples in our laboratory, and this figure has been increasing in the last few months.



As you can see in the graph, the most prevalent malware category in 2009 was that of Trojans (66%). They have held this position for the last few years, mainly due to their use for financial objectives. It is also relatively easy to obtain new variants, as Trojans and tools for creating Trojans are sold online.

Some way behind Trojans is the category of Adware (17.62%), which includes rogware or fake antiviruses. This is not surprising, as the use of these phony security programs has been increasing in 2009. However, it is unlikely they will overtake Trojans, even if they are also motivated by financial benefits.

However, it is a surprise to see viruses in third position at 6.61%. In recent years, this category was apparently losing ground, pushed back by Trojans and worms. Yet numerous virus infections have been observed in 2009, including those of Sality and Virutas. There have even been variants of Virutas that download and install crimeware onto computers (e.g. banker Trojans). The disinfection of this highly complex virus involves a considerable drain on the resources of antivirus companies. One theory behind the resurgence of viruses (particularly the complex ones), is that cyber-crooks want antivirus companies to focus on disinfecting viruses, so they dedicate less time to the malware designed to steal information. In any case, this strategy has clearly failed, as it has resulted in greater investment in anti-malware laboratories.

Next comes the category of spyware (5.70%) followed by worms (3.42%), yet the low ranking of worms belies the fact that 2009 has been the year of Conficker. This worm has caused serious problems in both domestic and corporate environments, and is still infecting computers worldwide.

At 0.65% the 'Other' category includes the following:

PUPs (Potentially Unwanted Programs)	57,10%
Hacking tools	38,41%
Dialers	4,23%
Security risks	0,26%

In short, the top categories (Trojans and adware) confirm the predominance of the new, financially-oriented, malware dynamic.

Trojans are largely focused on stealing bank details or other information and still represent a quick and simple way of obtaining money for cyber-crooks.

On the other hand, rogueware or fake antiviruses (adware) are also a serious threat to users, who are often taken in by the unorthodox techniques cyber-crooks use to defraud them.

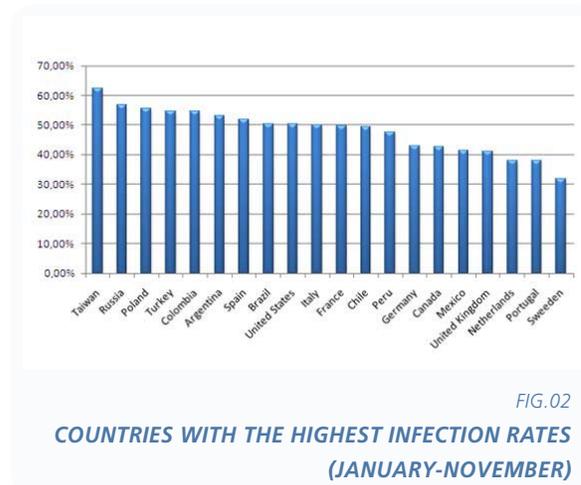
Global consequences of malware

The previous section looked at the distribution of the main malware categories based on the samples received by PandaLabs.

This section looks at the malware situation in several countries.

The data shown in the following graph has been obtained through analyses carried out by the online tool **ActiveScan 2.0**. This service allows any users to run free online scans of their computer, and check whether they are infected or not.

The graph below shows the countries with the highest infection rates:



The countries with most infections are Taiwan (62.20%), Russia (56.77%) and Poland (55.40%). Countries with the least infections include Sweden (31.63%), Portugal (37.79%) and the Netherlands (38.02%).

As we can see from the statistics of 2009, it has been an active year with respect to malware creation and infections. So how is this reflected in the real world? Is this something that affects us directly? Or are these just more figures that have little bearing on our lives? If we look back at what has happened during the year, it is evident that this really can affect us directly.

The harsh reality

In January, the Ministry of Defense in the United Kingdom acknowledged that it had fallen prey to **an infection which had impacted the Royal Navy**. Although no sensitive information had been exposed, naval warships had been affected, and were left without email or Internet communication.

In the same month, several hospitals in Sheffield, England suffered an attack that hit at least 800 computers. In February, it was revealed that three London hospitals **had lost network connectivity** due to infections at the end of 2008.

Just in 2009, more new malware appeared than in the entire history of computer viruses.

Also in February, computers at the municipal courts in Houston USA were infected by a virus, resulting in the suspension of several hearings. The local police force was even ordered to suspend arresting people for minor offenses.

In May, **part of the network of the US Marshals** (a division of the US Justice Department) had to be disconnected to remedy an infection.

These cases are not isolated events; they reflect what is happening in the world. The main lesson here is that many of these incidents could have been prevented with a series of basic security measures: from having an up-to-date antivirus on all computers, to implementing a policy of applying security patches.

That said, not all infections are the consequence of a lack of the appropriate security measures. Many stem from direct attacks on users who have not behaved in any way that could be considered a risk. In February, **readers of eWeek were victims of an attack** launched through an advertising banner provided by DoubleClick, a subsidiary of Google. In this case, cyber-criminals exploited the DoubleClick ad distribution platform to distribute malware.

A **similar attack** took place in September, this time targeting the New York Times, and **once again** in October on the Gizmodo blog.

Other types of attacks involve direct hacking of websites. In January the webpage of **the Indian Embassy in Spain was attacked**, and then used to distribute a dangerous backdoor Trojan to visitors. The same happened to the **Web page of Paris Hilton** in February, and to that of **ex-Beatle Paul McCartney** two months later. In this case the malware distributed was designed to steal bank details.

June saw the British Communist Party's website manipulated by Chinese hackers to distribute malware.

Repairing the damage caused by these types of attacks is costly. The Pentagon admitted in April that it had spent \$100 million over the last six months making good the damage done by cyber attacks and other related problems.

Total losses attributed to infections and hacker attacks are estimated at thousands of millions of dollars.

And this is not the only financial consequence. The bottom line is that cyber-crooks look to profit from their activities, and if they can do this by stealing money directly, then they do. Brian Krebs revealed in October how cyber-criminals have stolen **millions of dollars from small and medium-sized companies** across the United States over the last few months.

There have also been security breaches allowing cyber-crooks access to confidential user information. In February, it was revealed that a security hole in Citibank's systems on December 23, 2008 led to a **coordinated attack across 47 cities around the world**, with criminals taking no less than \$9 million from ATMs in just one day.

Once again we are not talking about an isolated case. A similar problem was uncovered in March, where **19,000 credit card numbers** (and other details) had been revealed. Another security breach in Network Solutions allowed hackers to monitor all operations between March and June, exposing the **details of more than 500,000 credit and debit cards**.

It's not all bad news

Having read down to here, some of you will perhaps be ready to pull the plug on your computer in an attempt to isolate yourselves from such cyber-delinquency. Yet there has also been good news this year in the fight against cyber-crime. March saw Romanian police **arrest 20 people on the suspicion** of being involved in a phishing scam. In the same month, police detained another individual suspected of hacking the US Defense Department in 2006, who now faces up to 12 years in jail.

Some might feel that these types of sentences are excessive, but what is the alternative? In 1998, Ehud Tenenbaum was arrested in Israel after having stolen credentials and infiltrated computers in Israel and the United States. Victims of his attacks included the US Defense Department, NASA and the MIT, as well as Web pages of the Israeli parliament and president. He was eventually sentenced to six months community service. What happens when the necessary measures are not taken in the face of these types of attacks? Criminals feel they can act with impunity, and even if they are caught, such light sentences mean that it has still been worthwhile. In August 2009, Ehud Tenenbaum was extradited to the United States accused of stealing more than \$10 million from different American banks. He was extradited from Canada, where he had been arrested in 2008 on suspicion of stealing \$1.5 million from Canadian banks.

It is essential that there is global cooperation to mitigate cyber-crime effectively.

A man was detained in London in September accused of stealing **more than 1 million pounds**. In October, 100 people were arrested by US and Egyptian security forces in **one of the biggest operations against cyber-crime** to date. They are accused of stealing more than \$1.5 million through phishing scams.

These are just a few of the arrests made during 2009. It is clear we are moving in the right direction, although there is still a long way to go, particularly in terms of international cooperation with countries such as China or Russia, from where a significant number of cyber-attacks are launched.

Social engineering, social networks and Web 2.0

For years, social engineering has been a technique favored by cyber-criminals for infecting users. And 2009 has been no different. In fact, the popularity of social networks has seen a resurgence in attacks that use these types of techniques. Let's not forget the scale on which these social networks are used; Facebook has over 350 million users, and Twitter continues to grow, with more than 15 million users in the United States alone. It is increasingly common for people to use these networks to communicate with friends instead of, say, by email. And cyber-crooks are well aware of this.

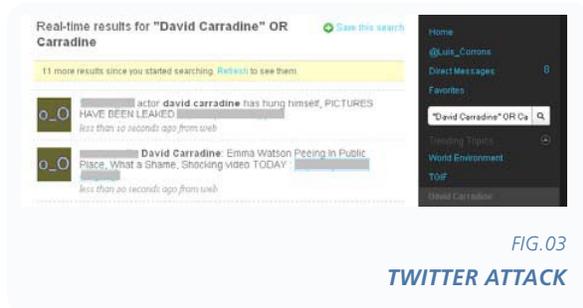
Twitter.

The enormous success of Twitter –the world’s leading micro-blogging tool- in 2009 has attracted the unwanted attention of cyber-criminals. In January, the accounts of 33 celebrities and public figures – including those of Britney Spears and Barack Obama-, had to be suspended after being hijacked and used to disseminate spoof information.

A worm appeared in April which used a cross-site scripting technique to infect Twitter users when they visited the profiles of other infected users. It then infected the new user’s profile to continue propagating. New variants of this worm soon emerged, created by one Mikey Mooney, who apparently wanted to attract users to a service competing with Twitter.

The popularity of Twitter has led cyber-crooks to see it as a valuable tool for propagating malware and spam.

In early June, Twitter was the focus of other attacks, this time using different techniques. Basically, BlackHat SEO techniques (which we will look at in more detail later) have been adapted to the Twitter environment. This social networking service has a feature called “Twitter Trends”, which is a list of the most popular topics on Twitter. When users select a topic through this feature, they will see all ‘tweets’ published related to this issue. As these are the topics that most people read, they make an obvious target for cyber-crooks.



In this case, malicious users were writing tweets about the topics listed in Twitter Trends with links to malicious Web pages from which malware was downloaded. The first attack we came across focused on just one of the topics, but just a few days later the scope of the attack increased and all popular topics contained malicious links. When the actor David Carradine died, in just a few hours there were hundreds of malicious tweets, and the same occurred with other popular issues on Twitter.

Facebook

As with Twitter, Facebook has become another popular target for cyber-criminals. Phishing attacks aimed at hijacking Facebook accounts have been particularly noticeable, with spoof Facebook sites designed to steal users’ account details.



There have been many other cases of fraud, such as the **scam detected in September** where users were offered the chance to hack other users' accounts – for a fee, of course:

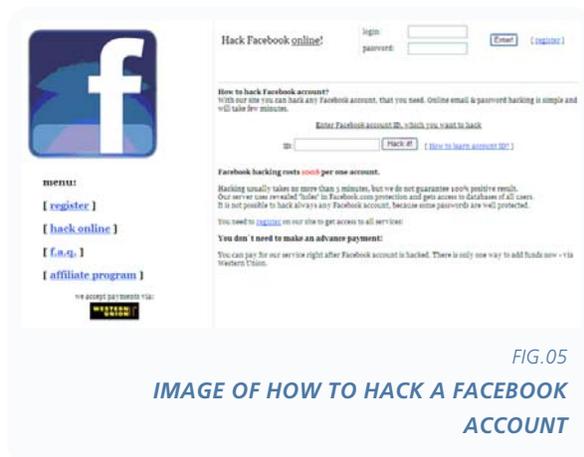


FIG.05

IMAGE OF HOW TO HACK A FACEBOOK ACCOUNT

Facebook was also the target of a specific family of malware –Koobface- which used this social network in order to spread. This worm has since evolved, and now uses new channels of propagation such as MySpace or Twitter. Several variants of this malware also install other threats –including banker Trojans and rogueware- on infected systems.

Web 2.0

In addition to social networks, there are myriad online services that adhere to the concept of Web 2.0, many of which have also become targets for cyber-crime.

In May, YouTube, the most popular video hosting site on the Internet, was the victim of an attack. YouTube lets registered users add comments to the pages displaying the videos. In this case, criminals created accounts and then generated a series of comments automatically. These comments **included links to malicious websites** designed to infect users. In total, more than 30,000 such malicious comments were created.



FIG.06

YOUTUBE ATTACK

Similarly, Digg.com was swamped with more than half a million malicious comments in just a few hours. Users that followed these links would be infected with rogueware:



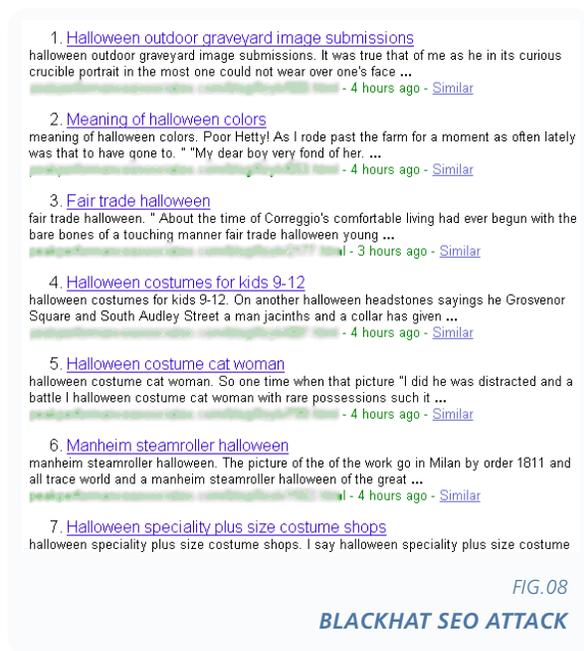
FIG.07

DIGG.COM ATTACK

BlackHat SEO techniques

SEO (Search Engine Optimization) refers to the techniques used to improve the positioning of Web pages in the results returned by search engines such as Yahoo, Google, etc. BlackHat SEO refers specifically to the use of SEO techniques by cyber-criminals to promote their Web pages.

Although BlackHat SEO attacks are nothing new, we have witnessed a significant increase in 2009. In April, we uncovered one of the largest BlackHat SEO attacks to date. Cyber-criminals created more than 1 million links in order to direct users searching with terms related to Ford to malicious Web pages. After we reported this attack, the campaign was changed to focus on searches for Nissan and Renault. Both cases operated in the same way: once users reached the malicious Web page, they were asked to install a codec to view a video. The codec however was really a fake antivirus called MSAntiSpyware2009.



Since then, similar cases have appeared using different subjects. It is important to underline the emphasis that cyber-criminals have given these techniques. They always use the very latest topics, taking advantage of tools such as Google Trends to find out exactly which terms Internet users are searching for, and they are quick to pick up on the latest news items, such as swine flu, etc.

On June 1 Microsoft announced in E3 its "Project Natal", the new system which allows interaction with Xbox 360 without the need for manual controls. This was a widely covered story. Less than 24 hours later, when searching Google with the words "Youtube Natal", the first result returned was a malicious Web page.

We have seen similar attacks throughout the year, using the death of Michael Jackson, Halloween, etc.

Cyber war: myth or reality?

While it's true that there have been attacks with clearly political motives, it would be more accurate here to talk about cyber-terrorism. Throughout 2009 we have seen numerous such attacks:

On January 18, a DDoS attack left the Asian republic of Kyrgyzstan **without Internet for more than a week**. All available evidence would suggest that the responsibility lies with the same Russian group that launched a similar attack in 2008 against Georgia. Coincidentally, the first large-scale attack of this kind was perpetrated in 2007 against Estonia, and once again the source of the attack was Russia.

Cyber-terrorism is real, and is on the increase. The Internet provides the anonymity needed to launch these types of attacks without being traced, yet most of these attacks appear to come from the same countries.

In February, a group based in China hacked the **web page of the Russian consulate in Shanghai**.

A few months later, in April, **the New York Police Department** revealed that its computers had been under attack; specifically, it had registered some 70,000 daily attempts to enter its network. The majority of these attempted hacks could be traced back to China.

In July, several websites belonging to the US and South Korean governments were the **targets of a DDoS attack**. Although it is yet unclear who was behind this activity, many are pointing the finger at North Korea.

Similarly, a series of government **websites in Poland came under attack** in September. Yet again, the attack could be traced back to Russia.

In October, the Swiss foreign ministry was the victim of a targeted attack by hackers.

It is clear then that these attacks are more than just anecdotal: we are facing a real situation. The Obama administration, aware of the danger of not having a coordinated structure to deal with these issues, placed Melissa Hathaway in charge of a review, the result of which was the creation of a national plan to combat cyber-crime.

In this plan, the President acknowledges that there are too many players involved in the management and resolution of incidents resulting from cyber-terrorist attacks, and yet a lack of coordination at the right level. To this end, the plan contemplates the creation of a 'cyber czar', directly answerable to the White House, and responsible for coordinating all agencies related to cyber security, and taking overall charge in the event of a real threat to the country.

Similarly, a budget has been made available to develop a series of initiatives designed to prevent risk situations. The President has urged the industry and other relevant agencies and organizations to collaborate in a plan that is set to mark a turning point for Internet regulation, while at the same time respecting the rights of individuals with respect to freedom of speech and the protection of privacy and personal data.

Other countries are also getting to work, with working groups and associations with similar aims to those of the USA: ensuring national stability in the event of cyber terrorist attacks.

This is the case in Spain, with the National Cyber-Security Advisory Council (**CNCCS**), which brings together the country's major security developers in close collaboration with government agencies. It operates on two main fronts: fomenting cooperation between organizations, developers and service providers to improve security for the general public and delivering initiatives aimed at improving and increasing training and education in cyber-security.

In December, the USA and Russia began talks on restricting the development of cyber-weapons. While this in itself will not mitigate the problem, it may lead to an international treaty that facilitates the fight against cyber-crime by the authorities in each country.

Before the end of the year, the Obama administration appointed the person who will coordinate US cyber-security and launch the plan aimed at improving not only American security, but also global security: Howard A.Schmid

The profitability of rogueware

Rogueware or fake antivirus products have been a major talking point in 2009. Although these applications have been in circulation for several years, it wasn't until the beginning of 2008 that they began to be used on a massive scale.

These are applications that purport to be antivirus products, detecting numerous (non-existent) threats on victims' computers. When users go to remove the threats, they will be asked to buy the 'full' product license.

All the while, pop-up messages will warn users of the danger they face, once again with the aim of coaxing users into paying for the license, either out of fear or frustration.

Every day, more rogueware appears in circulation, much of it practically identical to other variants: the same icons, interfaces, warnings... all that changes is the name.

Where previously the techniques used by this type of malware were more annoying than dangerous, recent examples have become more aggressive.

Such is the case with **TotalSecurity2009** which, having infected a computer and after the system is restarted, prevents users from running any file on the computer. When users try to open any file, a pop-up message appears claiming that the file is infected.

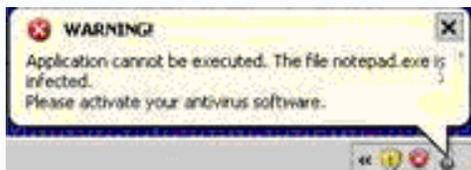


FIG.09

MESSAGE DISPLAYED BY TOTALSECURITY2009

It also changes the desktop wallpaper, inserting a warning claiming that the computer is infected and recommending the action to take to remove the threats.

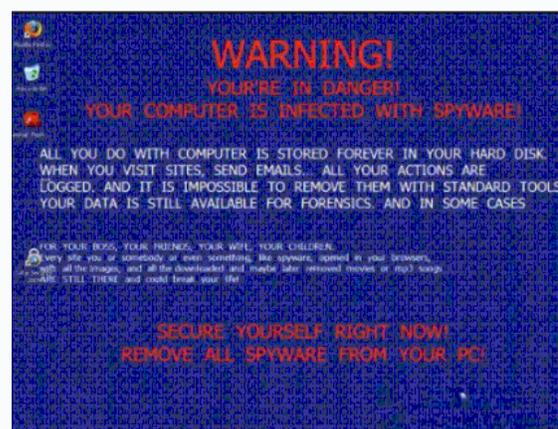


FIG.10

DESKTOP WALLPAPER DISPLAYED BY TOTALSECURITY2009

Another technique which is now used by some of these programs is to display a screen similar to the Windows Security Center. The text on this screen informs users that no antivirus protection has been detected on the system, other than an unregistered version of the (fake antivirus) program. There are several links through which users can buy the rogueware license.

The example below shows **PersonalProtector** which, when run, displays the following fake Windows Security Center screen:



FIG.11

IMAGE IMITATING THE WINDOWS SECURITY CENTER

The image below shows the amount of rogware received at PandaLabs throughout the year:

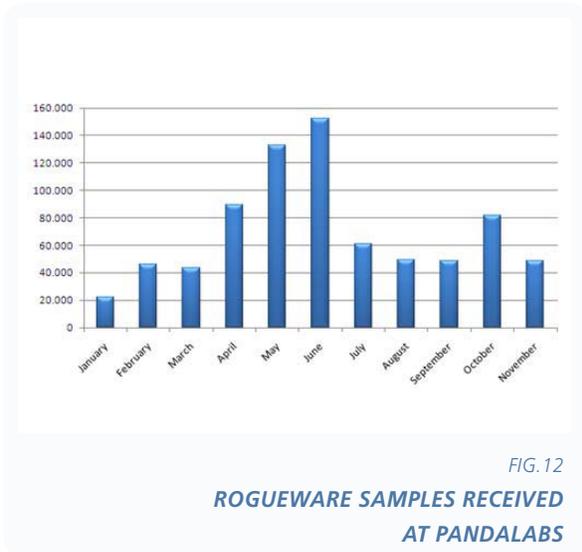


FIG.12

ROGUEWARE SAMPLES RECEIVED AT PANDALABS

During Q1, the number of examples of rogware received at our laboratory was relatively low. This increased rapidly from April on, and peaked in June with more than 140,000 examples. The number then dropped sharply during the rest of the year, with the exception of another sharp rise (80,000 examples) in October.

Although the figures for recent months are comparatively low, bear in mind that just in the last two months we have received more new variants than in the whole of 2008.

These are the global figures, but now we're going to look at the most active rogware family during 2009.

This is illustrated in the following image:

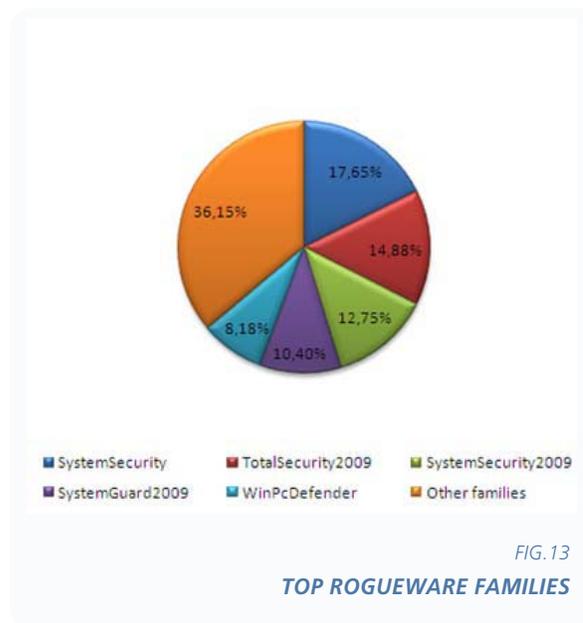


FIG.13

TOP ROGUEWARE FAMILIES

It is clear that the most active rogware family during 2009 has been **SystemSecurity**, which accounted for 17.65% of all infections, followed by **TotalSecurity2009**, with 14.88%. As mentioned above, this family is characterized by the aggressive techniques it uses to force users to buy. Then come **SystemSecurity2009**, with 12.75%, **SystemGuard2009**, with 10.40% and **WinPcDefender**, with 8.18%.

The remaining rogueware families are included in the 36.15% accounted for by "Others".

It would seem that cyber-criminals have really hit the jackpot with the distribution of these programs, and while they continue to return such profits, rogueware will continue to proliferate. According to a study by PandaLabs, cyber-crooks are earning more than \$400 million a year with this technique.

Banker Trojans

Banker Trojans are still among cyber-criminals' favorite tools for stealing confidential information from users. These programs are readily available to cyber-criminals, as there is an extensive black market in a la carte Trojans and banking malware kits. These kits allow users not only to create Trojans with multiple functionalities but also to control them and even send them new instructions.

However, an increasing number of banks are implementing advanced security measures to prevent the theft of information from clients. Consequently, criminals are having to design increasingly sophisticated malware to evade these measures.

Nevertheless, it is not just down to the banks; users must also be aware of the precautionary measures to take to prevent banker Trojans from infecting their computers. For this reason, cyber-criminals still favor the use of social engineering techniques.

End-users are still the weakest link in the chain and therefore the main target of criminals.

Although most banker Trojans use similar techniques to steal information, this year we have seen some examples that have become particularly sophisticated, such as **SilentBanker.D**.

This uses a technique whereby when an infected user makes a bank transfer, the Trojan is able to edit the details of the recipient so that the money ends up in the criminal's bank account. What's more, the user is unaware of the theft as the receipt shows the name of the intended recipient.

This in itself is not new, yet this Trojan goes one step further, as it remains resident on the victim's computer, falsifying online bank statements to the effect that unless users go to their bank's offices, they will be unaware of the theft.

Banker Trojans in general, along with rogueware, are now the most profitable category of malware for cyber-criminals.

2009: The year of Conficker

Conficker has been without doubt the most significant malware during 2009, not just because of the media attention it attracted or the number of computers infected worldwide, but also because it represented a leap back in time to the era of massive virus epidemics.

Security experts estimate that Conficker has already infected more than 7 million computers around the world.

More than a year has passed since Conficker first appeared, yet it is still making the news. The patch for the vulnerability exploited by Conficker (MS08-067) was published by Microsoft in October 2008.

Yet more than one year later, Conficker continues to infect computers.

So why is this still happening?

Principally, because of its ability to propagate through USB devices. Removable drives have become a major channel for the propagation of malicious code, due to the increasing use of memory sticks and portable hard drives to share information (in households and corporate environments).

Nowadays, most companies have perimeter protection (firewall, etc.), but this does not prevent employees from taking their memory sticks to work, connecting them to the workstation and spreading the malicious code across the network. As this worm can affect all types of USB devices, MP3 players, cell phones, cameras, etc. are also at risk. To mitigate this threat, users need tools such as **the free USB vaccine** we launched in 2009, protecting not just the computer but also the USB device itself.

Another reason for the longevity of this worm is that many people are using pirated copies of Windows, and in fear of being detected, they avoid applying the security patches published periodically by Microsoft. In fact, Microsoft allows unrestricted application of critical updates, even on non-legitimate copies of its operating system.

The spread of Conficker impacted all types of institutions and organizations. Victims included the British and French military, as well as universities such as Utah in United States.

Microsoft even offered a reward of \$250,000 to anyone providing information that led to the arrest and conviction of the creators of this malware.

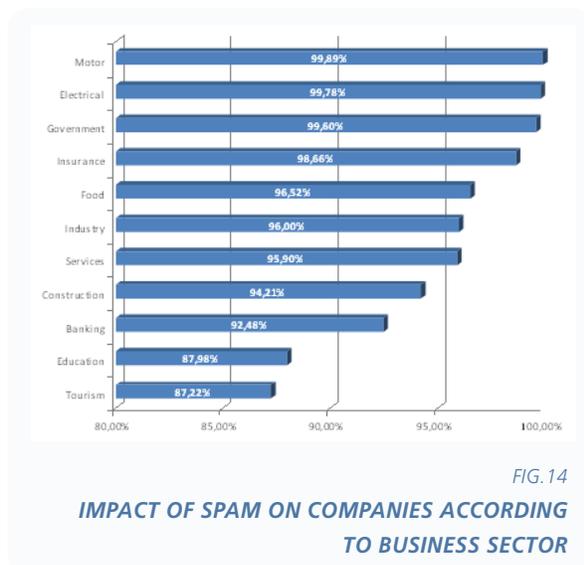


Spam figures have remained very high over the last year: in 2009, 92% of all email worldwide was spam. As we have often pointed out, spam has a number of objectives, from the sale of illegal products, to the redirection of web traffic to spoof Web pages used to infect computers, and even direct distribution of malware.

We carried out a study in 2009 of how spam was affecting the industrial sector. This involved a detailed analysis of the email traffic of 867 companies from 11 different sectors and across 22 European and American countries. In total, over 2,000 million messages were analyzed.

The aim of the study was to determine the impact of spam and malware on companies according to business sector.

The main conclusion of the study is that the **automobile** and **electrical sectors**, followed by **government institutions**, comprise the top three recipients of spam and email-borne malware with ratios of 99.89%, 99.78% and 99.60%, respectively. These figures represent the amount of spam or malicious messages as a percentage of all email traffic at these companies. Alternatively, just 0.11% of email received by companies in the motor industry is legitimate (0.22% and 0.4% for the electrical and government sectors respectively).



Interestingly, the **banking** sector, which would seem to be a prime target, features near the bottom of the ranking with a ratio of 92.48%. The **education** and **tourism** sectors close the ranking with figures of 87.98%, and 87.22%.

There was, however, no considerable difference in the subject fields of the spam received across the various sectors. The majority, more than 68%, were related to pharmaceutical products. This was followed by adverts for replica products with 18%, and messages with sexual content at 11%.

Banker Trojans accounted for most of the malware received, being the culprit in 70% of detections. This was followed by adware/spyware, at 22%, with the remainder taken up by viruses, worms, etc.

Throughout 2009 there have been numerous incidences of spam-borne malware attacks:

- The use of topical issues or shocking news stories, whether true or not, continues to be a popular ruse for spreading malware in spam messages.

In January 2009, banker Trojans were distributed in spam messages carrying **a CNN story about the conflict in Gaza**. The messages contained a link pointing to a spoof CNN Web page offering more information and, supposedly, a video. Users that tried to play the video would see a message telling them to update Flash Player and offering them the option to download a new version. Any users that opted to download the application would really be downloading and running the Trojan.

Also in January, we saw the Waledac worms distributed in spam messages using similar social engineering techniques. This time the message claimed to contain a story about Barack Obama turning down the presidency of the United States. To make it more credible, users that wanted to read more were redirected to what appeared to be the official Web page of the President.

In February it was the turn of Tony Blair. Spam messages containing banker Trojans claimed that the **ex-Prime Minister of the United Kingdom had died**. Once again the messages contained a link supposedly to a news agency, in this case the BBC. And as before, users were asked to download a more recent version of Flash Player in order to see a related video.

The news of the death of Michael Jackson had a major impact around the world, not just the story itself but also speculation about the cause of death. Needless to say, spammers were quick to take up the opportunity to distribute malware. Rumors about the possibility that he had been murdered quickly led to a stream of spam messages such as the one below:

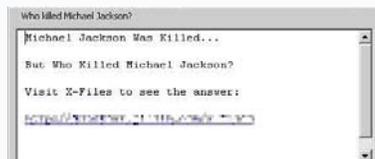


FIG. 15

SPAM MESSAGE ABOUT MICHAEL JACKSON'S DEATH

- Another strategy frequently used by criminals to distribute malware is the sending of messages containing invoices for products that users have supposedly bought over the Internet, such as airline tickets, or non-delivery messages claiming to be from parcel delivery services.

In January, several attacks distributed Trojans in messages seemingly from **US airline companies**. The attachment to these messages contained a spoof flight ticket, supposedly bought by the user. The ruse centered around making users believe that their credit cards had been used fraudulently.

Throughout the year we have detected spam messages that claim to have been sent by parcel delivery companies, such as UPS or DHL, informing users that a packet could not be delivered because of problems with the address and asking them to open and print an attachment, needed, so the message claims, to collect a parcel:



FIG. 16

SPAM MESSAGE THAT USES DHL DELIVERY COMPANY

- Finally, we can't fail to mention one of the biggest stories of 2009: swine flu. This serious issue has generated, and continues to generate, considerable concern around the world. It is no surprise then that cyber-crooks were quick to exploit the subject for their own malicious purposes.

In December, email messages claiming to contain information about the virus were used to distribute banker Trojans. These messages supposedly offered **details of an H1N1 vaccination program**, asking users to create their personal vaccination profile on a certain Web page. The messages contained a link to the website.

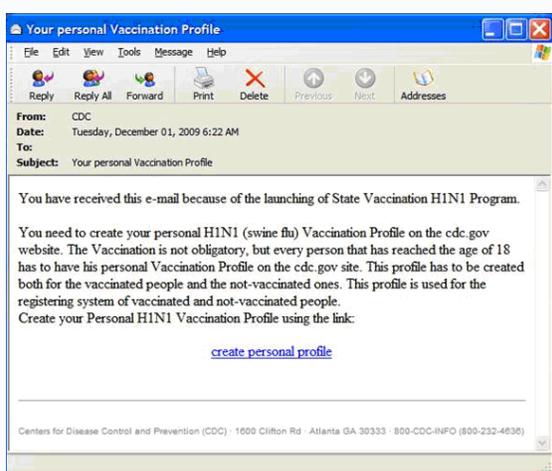


FIG. 17

SPAM MESSAGE ABOUT THE SWINE FLU

The year 2009 started off with several public exploits for vulnerabilities in Oracle products. The most serious flaw -by the number of affected computers- (CVE-2008-5457) impacted all J2EE Bea WebLogic application servers. This flaw could be exploited remotely with no need for a user name and password, which gave it a 10/10 severity rating in the **CVSS2** scale. As a result, attackers could remotely take control of the computer(s) that hosted the application server.

It was not until May that another serious flaw appeared. On this occasion, a bug was discovered that affected all Microsoft Internet Information Servers with WebDAV enabled. Through this vulnerability (CVE-2009-1535), an authenticated attacker could access files that, otherwise, would not be accessible to them. That is, the flaw offered a way to bypass authentication and validation when accessing resources.

The rest of the year saw the appearance of the usual vulnerabilities in popular products such as browsers, office application suites, etc.: Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Adobe Acrobat Reader (more on this later), Microsoft Office, OpenOffice, Fox IT Reader, etc. The number of flaws detected in these products is alarming but not surprising, as these applications have reached such complexity that entering new bugs is much easier than in simpler software. The more complex the software, the easier it is to find a flaw in it.

However, the most serious vulnerability of 2009 was discovered in September (CVE-2009-3103). Laurent Gaffié reported, in Full Disclosure, a bug that he misclassified as just a denial of service attack. Had this been true, the bug would have been nothing more than a mere nuisance. However, it was an extremely serious flaw that affected Vista and all later Microsoft Windows versions. The vulnerability allowed the remote execution of code with authentication at kernel level.

The researcher Rubén Santamarta published more technical details about this vulnerability just one day after Laurent Gaffié reported it. The flaw was a classical example of "out-of-bounds dereference". The flaw lay in an array index error in the SMBv2 protocol implementation in srv2.sys in Microsoft Windows Vista Gold, SP1 and SP2, Windows Server 2008 Gold and SP2, and Windows 7 RC. The vulnerability allowed remote

attackers to execute arbitrary code or cause a denial of service (system crash) via an & (ampersand) character in a Process ID High header field in a NEGOTIATE PROTOCOL REQUEST packet. This triggered an attempted dereference of an out-of-bounds memory location, aka SMBv2 Negotiation Vulnerability.

The flaw took quite a long time to be exploited, which, in this context usually means less than one day. The first ones to claim they had created a viable remote exploit to take control of affected computers were the American researchers Immunity Sec. More specifically, it was Kostya Kortchinsky who wrote the complex exploit. This exploit was exclusively offered to their clients.

The company whose products have been subject to the largest number of exploits this year is Adobe. Adobe clients have also been those that have been exposed to flaws for the longest time. In all, 45 vulnerabilities have been reported in software belonging to this company this year. Compared to other software packages, such as Microsoft Windows (the entire operating system and basic applications), 41 vulnerabilities have been fixed in the Adobe (Acrobat Reader and Flash Player) software. That is, more vulnerabilities than in an entire operating system. Also, the time window during which Adobe users have been vulnerable to exploits has exceeded 30 days in the majority of cases. The latest example of this is the 0-day vulnerability discovered in Adobe Acrobat Reader just 2 days before starting to write this article. Undoubtedly, this has been a year forget for Adobe.

More clouds on the security horizon

Welcome to the cloud. In 2007, we launched our first product which took advantage of the cloud, now in 2009 all our products use it and we have launched the first 100% cloud-based antivirus: CloudAntivirus. We have also seen this year how other major security vendors have followed our steps and taken to the cloud. 2010 will be the year in which all anti-malware companies wanting to offer real-time protection will have to follow suit. And those that don't will be out of the game.

An avalanche of malware

The amount of malware in circulation will continue to grow exponentially. The greater speed delivered by cloud-based technologies, such as Panda's Collective Intelligence, will force malware creators to generate even more threats in order to evade detection and elimination. Once again malware will be designed almost exclusively for financial gain, and we can expect to see many new fake antiviruses (rogueware), bots and banker Trojans.

Social engineering

Cyber-criminals will again be focusing on social engineering techniques to infect computers, particularly those targeting search engines (BlackHat SEO) and social networks, along with 'drive-by-download' infections from Web pages.

Windows 7 will have an impact on malware development

Where Windows Vista hardly caused a ripple, Windows 7 will make waves. One of the main reasons is the widespread market acceptance of this new OS, and as practically all new computers are coming with Windows 7 64-bit, criminals will be busy adapting malware to the new environment. It may take time, but we expect to see a major shift towards this platform in the next two years.

Cell phones

Will 2010 be the year of malware for cell phones? Several security companies have been warning for some time that malware is soon to affect cell phones in much the same way as it affects PCs. Well, we hate to rain on their parade, but 2010 **will not** be the year of malware for cell phones. The PC is a homogenous platform, with 90% of the world's computers are running Windows on Intel, meaning that any new Trojan, worm, etc. has a potential victim pool of 90% of the world's computers. The cell phone environment is much more heterogeneous, with numerous vendors using different hardware and different operating systems. Applications are sometimes not even compatible from one OS version to another.

So it is once again unlikely that 2010 will see widespread targeting of cell phones by malware. In any event, this year will witness many changes in the world of mobile telephony, with more smartphones offering practically the same features as a PC; the emergence of Google Phone –first phone sold directly by Google without tying users to specific operators-; the increasing popularity of Android, not to forget the success of the iPhone. If in some years there are only two or three popular platforms, and if people begin to operate financial transactions from their cell phones, then maybe we could talk about a potential breeding ground for cyber-crime.

Mac

Mac: has the danger arrived? Mac's market share has increased in recent years. Although the number of users has yet to reach the critical mass required to make it as profitable as PCs for cyber-criminals, it is nevertheless becoming more attractive. Mac is used just as PCs are to access social networks, email, the Internet... and these are the main malware distribution systems used by cyber-criminals. Consequently, Mac is no longer a safe haven against malware. These criminals can easily distinguish whether a system is Mac, and they have malware designed especially to target this OS. In 2009 we have already seen numerous attacks, and there are more to come in 2010.

The Cloud

Cloud-based services are not just used for security. We are all using more services delivered from the cloud, often without realizing. Who doesn't use Hotmail or Gmail as their email service, or Flickr to store photos? But cloud-based services are not limited solely to storage, they are also used for processing data. The cloud is a tool that can help save considerable costs for companies, and as such is rapidly growing in popularity. This makes attacks on cloud-based infrastructure/services far more likely.

Cyber war

Although this term is more associated with science fiction than the real-world, it's a phrase we are about to start hearing more often. Throughout 2009, governments around the world including the United States, the UK and Spain, have expressed concern about the potential for cyber-attacks to affect economies or critical infrastructure. We also saw this year how several Web pages in the United States and South Korea were the subject of attacks, with suspicion –as yet unapproved- pointing at North Korea. In 2010 we can expect to see similar politically-motivated attacks.



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/>

