



**QUARTERLY
REPORT
PandaLabs
(APRIL - JUNE 2008)**

© Panda Security 2008

PANDA
SECURITY

One step ahead.

Index

Introduction	3
Executive summary	4
Second Quarter Figures	5
Distribution of the new threats detected	5
Month by month	7
Threats detected by the PandaLabs sensors	8
Active malware	10
Q2 trends: infecting web pages	14
How do these attacks work?	14
Cases	15
Vulnerabilities	16
Summary	16
Microsoft Access and its vulnerabilities	16
Flash vulnerabilities: a growing problem	17
Banker Trojans	18
Most active families	18
Trends and conclusions	20
Spam and Phishing situation	21
Spam status in Q2	21
Distribution of spam on social networks	22
Phishing Kits / Fake Pages	24
About Pandalabs	32

Introduction

Here we present the Q2 report, which takes a look at some of the most interesting events of this quarter.

Banker malware continues to be one of the most worrying types of threats, and they are a growing trend. These types of threats, specialized in stealing passwords from different online banking services, continue to account for a large part of the profits generated by cyber-crooks. In this report we will look at the current situation of this category of threat and analyze the main families.

Yet banker malware is not the only source of business for Internet criminals, there is also spam and in particular phishing, another major source of income. We will be analyzing the reasons why spam and phishing are still successful criminal business models.

We will also look at another trend that has become increasingly prevalent this year: the infection of legitimate web pages to distribute malware. In this quarter, millions of legitimate web pages have been infected with malicious code.

We will also present the evolution of active malware by country throughout the year so far.

Similarly, as in previous reports, we will describe the most serious vulnerabilities detected this quarter and offer a statistical analysis of malware activity over the last three months.

We hope you find it interesting.

Executive summary

There are currently thousands of variants of single families in circulation in order to make detection more difficult and consequently lull users into a false sense of security.

The average infection rate over the first six months of the year has been 17.07%, an increase on the 15.87% recorded during 2007.

Spain, Mexico, Brazil, Colombia and Russia are the countries with the highest percentages of active malware over the year so far.

The infection of web pages as a method for distributing malware has been one of the leading trends of 2008.

This quarter has seen millions of legitimate web pages infected in order to infect users' computers with malware.

Banker malware increased more than 400% in 2007, causing financial losses to users around the world.

During the first months of 2008, spam levels fluctuated between 60 and 94 percent of all email sent across the Internet.

Second Quarter Figures

Distribution of the new threats detected

The graph below illustrates the distribution of new variants by type of malware detected by PandaLabs in the second quarter of 2008:

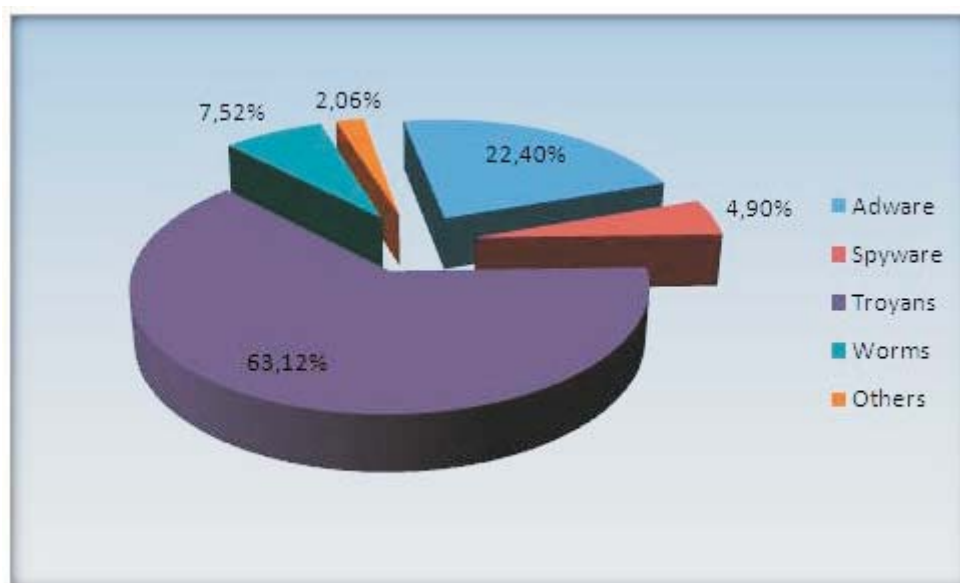


Figure 1. Malware detected in Q2.

As illustrated in the graph, the predominant malware category in Q2 has been Trojans, up nearly one point with respect to the previous quarter, at 63.12%.

The reason behind the dominance of Trojans is related to the new objectives of cyber-criminals, who are no longer trying to cause headline-grabbing epidemics but to infect systems silently. Yet, instead of trying to infect thousands of computers with one strain of malicious code, they distribute thousands of variants of one family. This makes them more difficult to detect, lulling users into a false sense of security.

Note that backdoors, a subclass of Trojans, have been integrated within these, and bots have also been integrated within worms and Trojans accordingly.

Second Quarter Figures

The percentage of worms has also increased slightly, now accounting for 7.52% of all malware.

Malware creators are still focusing heavily on hybrid worm-Trojans, used to obtain confidential information from systems.

We have grouped categories with low prevalence under the heading Others.

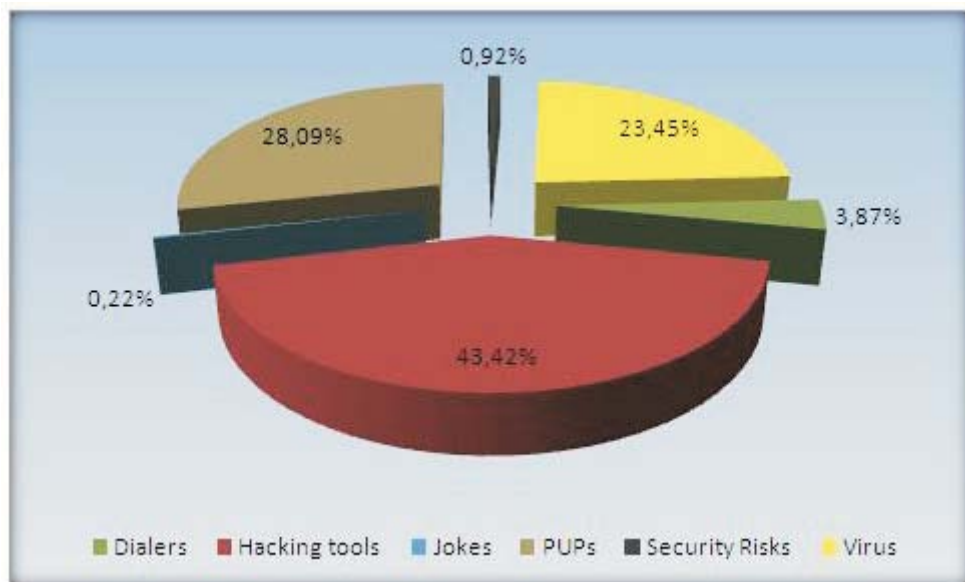


Figure 2. Other malware

Hacking tools and PUPs (potentially unwanted programs) are the leading malware in the Others section, at 43.42% and 28.09% respectively, followed by viruses with 23.45%.

However, the increase in users with broadband connections means that dialers are decreasing quarter by quarter.

Second Quarter Figures

Month by month

Below you can see the appearance of new malware month by month, separated into the most important categories. As you can see, the most prevalent category is Trojans.

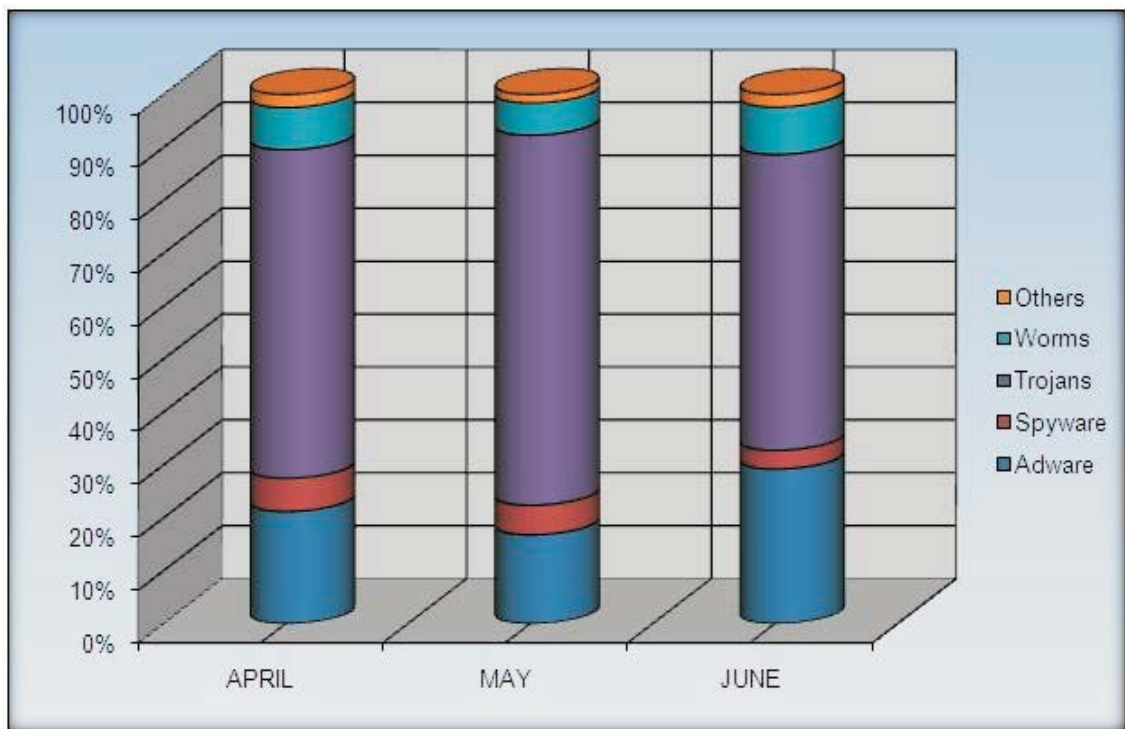


Figure 3. Monthly evolution

The most prevalent malware categories each month are those that provide the largest financial return to threat creators.

Second Quarter Figures

Threats detected by the PandaLabs sensors

The following graph shows the distribution of detections made by the Panda Security sensors throughout the second quarter of 2008.

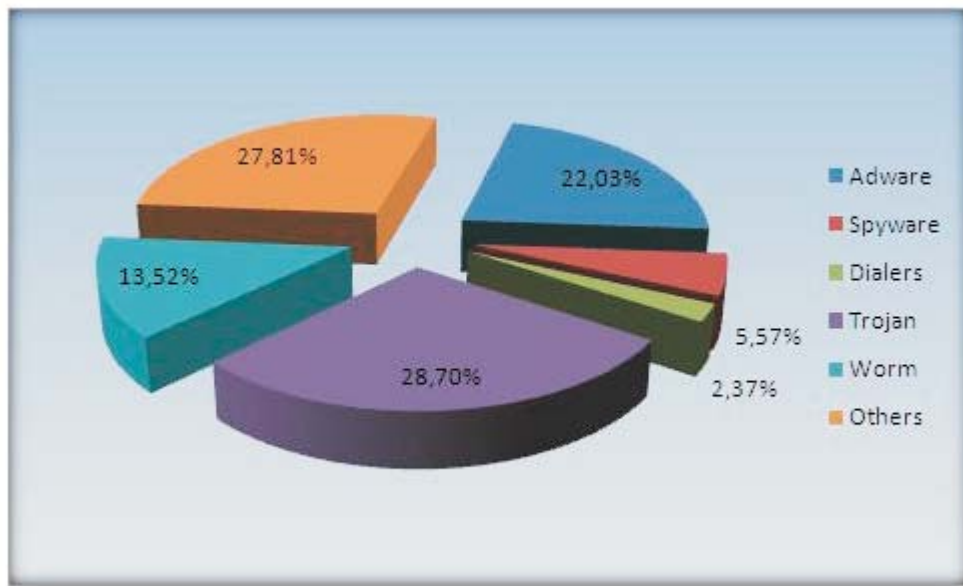


Figure 4. Malware distribution by categories

In this quarter, adware has decreased 6.55%, leaving first position to Trojans (28.70%), which have increased 3.24% with respect to the previous quarter, and are once again the most frequently detected type of malware.

Worms, with 13.52%, have increased 3.58% in the last three months.

Dialers dropped slightly to 2.37%, and still refuse to disappear, despite their downward trend all through last year.

Second Quarter Figures

Below you can see the 10 threats most frequently detected by these sensors:

01	W32/Bagle.RP.worm
02	W32/Puce.E.worm
03	W32/Bagle.SP.worm
04	Adware/AdsRevenue
05	W32/Perlovga.A.worm
06	W32/Bagle.KV.worm
07	Adware/Maxfiles
08	Trj/Dropper.UN
09	W32/Whybo.I.worm
10	Trj/Rebooter.J



Figure 5. Top ten of detected threats

Active malware

In this section we will be looking at how malware has evolved so far during 2008.

In order to understand what active malware is, we must first define the two possible statuses for malware: active and latent.

Latent malware is malware that is on a PC but not taking any action. It is waiting to be executed, either directly by the user or remotely by an attacker.

Once it is run, it starts to take the damaging action for which it has been programmed. In this case, the status changes from latent to active.

We have been monitoring the evolution of active malware month by month on our website: www.pandasecurity.com/infected_or_not/.

This service allows any users to run free online scans of their computer, and check whether they are infected or not.

The screenshot shows the 'Infected or Not?' web page. At the top, the title 'Infected or Not?' is displayed in red and blue, with the 'PANDA SECURITY' logo in the top right corner. A central figure of a man in a dark suit stands on a blue circular base, pointing towards a blue box on the right. The box contains the text: '23% of PCs with updated antivirus are infected* ...is yours?' and 'Scan your PC and find out!'. Below this box, it says '*Source: Panda Security Research 2007'. To the left of the man is a navigation menu with 'Home' and three categories of users: 'users' (with a yellow bar), 'users' (with a red bar), and 'users' (with a red bar), followed by 'Other antivirus users'. At the bottom, there are three call-to-action buttons: 'SCAN IT NOW' for 'ENTERPRISES' (with a 'Scans your network.' subtext), 'SIGN UP HERE' for 'CHANNEL PARTNERS' (with a 'Sign up to our channel partners program' subtext), and 'SCAN YOUR PC' for 'HOME USERS' (with a 'Scan your PC now.' subtext). The footer contains links for 'Blog', 'Panda Security Research', and 'Choose Country', along with copyright information: '© Panda Security 2008 | Privacy Policy | Legal Notice | About Panda'.

Figure 6. Infected or Not web

Active malware

The data compiled through the Infected or Not website can be consulted through the global infection map. By default, users will see statistical data for their country (the information below the map), but can also consult data for any other country by clicking on it and then on "View statistics". If you want to check the Worldwide infection data just click here.

In this graph you can see how malware has evolved so far during 2008.

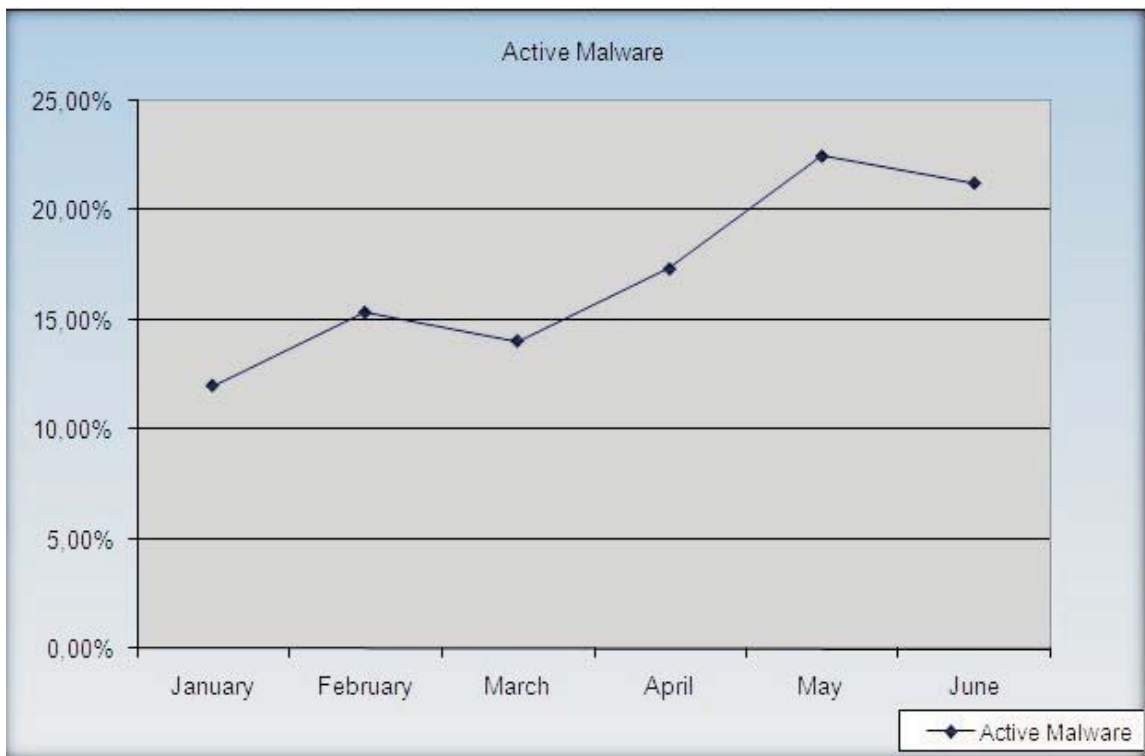


Figure 7. Evolution of active malware during the first semester

The data here shows that 2008 began with one of the lowest active malware infection rates (12%), only February 2007 was lower –with 8.53%. Since then, there has been a steady increase, with the highest rates occurring in May (22.48%). The average over the first six months of the year has been 17.07%, an increase on the 15.87% recorded during 2007.

Active malware

This data reflects the evolution globally, but what about in each country? In the following graph you can see the infection rates in the countries with the highest percentages of active malware.

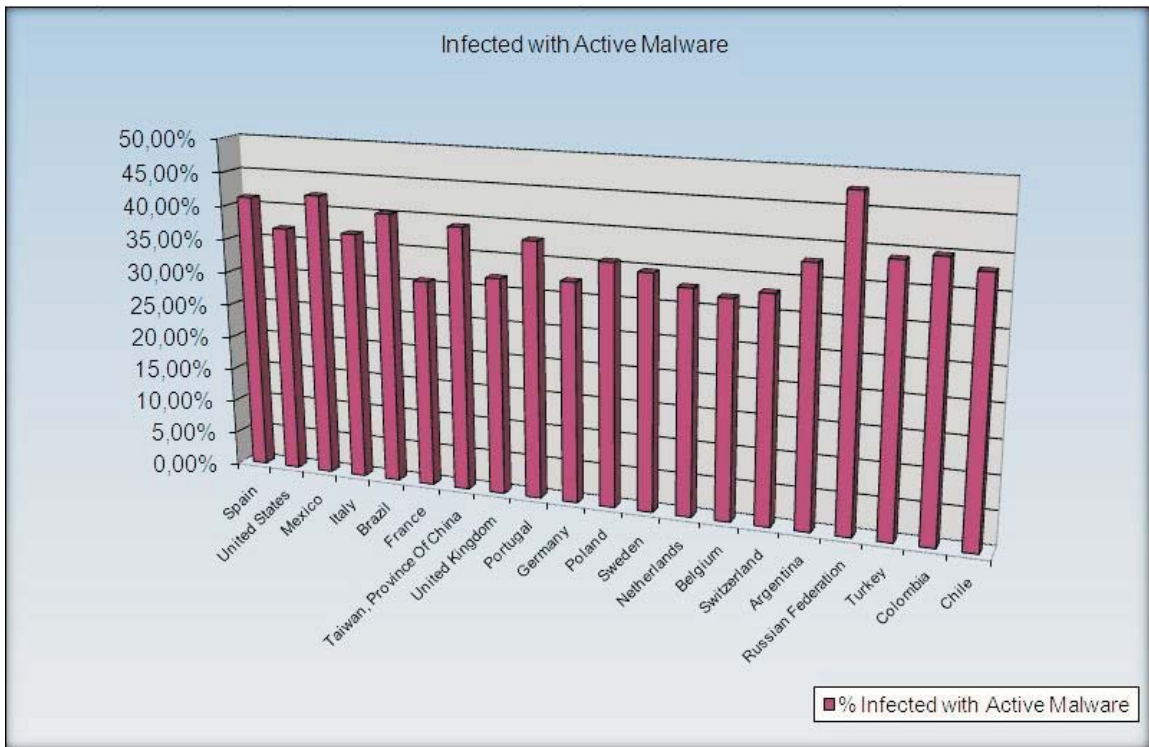


Figure 8. Countries with the highest percentage of malware

The graph shows those countries with the highest rates of active malware, with Russia clearly topping the list in the first half of the year with a rate of 47.67%. Spain, Mexico, Brazil and Colombia all had active malware infection rates around 40%.

With respect to specific types of malware, the W32/Bagle.RP.worm was the most active strain globally. In Brazil, however, banker Trojans were among the most active types of malware, with Trj/Banbra.FSY topping the list.

Active malware

Finally, it is worth noting the appearance of the [Exploit/iframe](#), which we mentioned in the PandaLabs blog. This malware has infected millions of legitimate web pages, and has been one of the most talked about IT security issues of this quarter.

The following diagram illustrates how these types of attacks operate.

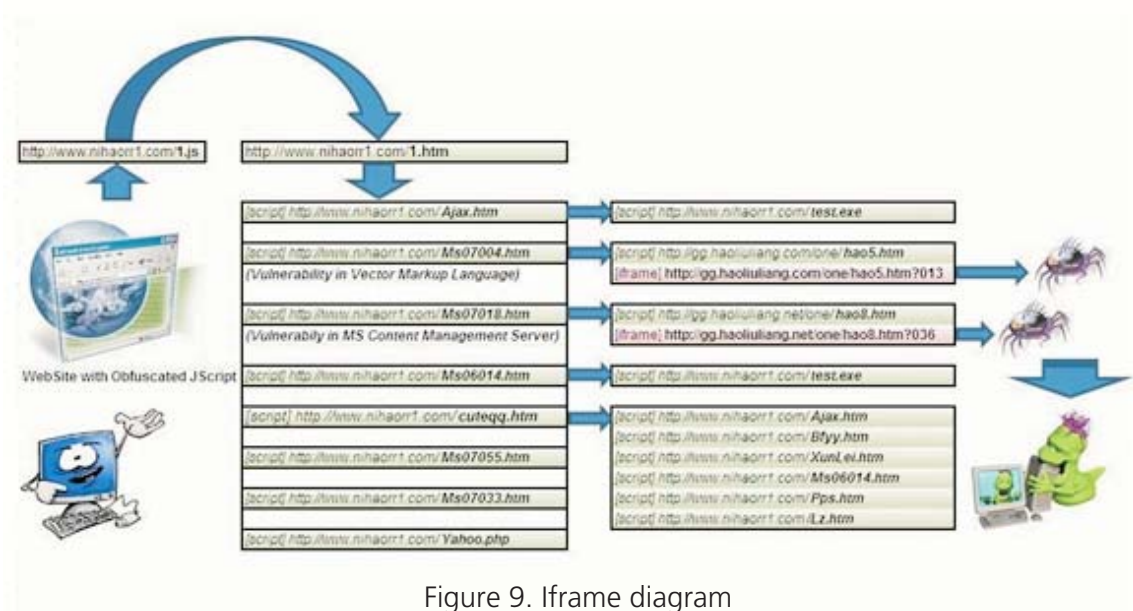


Figure 9. Iframe diagram

Q2 trends: infecting web pages

As predicted at the beginning of the year, web page infections as a means of distributing malware are a growing trend in 2008, especially in Q2.

This method has many advantages for cyber-crooks. First, if they manage to infect web pages with a large number of visitors, they do not need to 'publicize' the infected pages through spam, etc. since users directly access the infected page. Users' suspicions are allayed –as they don't fear being infected on trusted sites- and cyber-crooks' cut their own costs. Consequently, users can be infected even if they have avoided accessing unsafe pages.

This method is 'cleaner' since users are not required to carry out actions such as downloading files, etc.

In Q2 we have witnessed several attacks that have infected millions of legitimate web pages

How do these attacks work?

Cyber-crooks can infect web pages in several different ways. The first involves exploiting vulnerabilities in the software installed on a server, the second, through bad configuration of the programs installed and running, and the last, by stealing passwords for accessing the server using Trojans. These three techniques allow cyber-crooks, in addition to infecting the corporate website, to use the servers for a range of malicious actions, including hosting a program designed to infect visitors, distributing spam or storing stolen data.

Once they manage to access the web page, cyber-crooks add an iframe-type reference at the end of the file loaded by default, which indicates the malicious server. It usually indicates a PHP or JS script run on the attacked computer to select the best vulnerability for entering malware on the computer.

Q2 trends: infecting web pages

This tool could be installed on the same server. Malware hosted on third-party servers is more difficult to locate. Malicious tools have been found that install malware from web pages that can be 'activated' from thousands of different pages.

There is also a growing trend for exploits used to infect users. At the beginning, operating system exploits were used. The downside of using exploits is that users with patched operating systems are not infected, unless a zero-day exploit is used. Consequently, hackers came up with new ways of using exploits. In addition to the operating system, they started to include Internet Explorer exploits (the browser with the highest market share). As Firefox became popular, it was also included in the targets list. Next came the applications most commonly used by users, such as, Windows Media Player, Quick Time and Acrobat.

Cases

Such an attack took place at the beginning of May and affected over 200,000 Web pages. A problem in an asp page allowed a malicious iframe to be inserted on hundreds of thousands of pages.

A few weeks later, a similar attack was detected in which the URLs the malware redirected users to had been modified. Most of them were hosted on Chinese servers. Even though the number of affected pages was low, the attack was highly dangerous.

Vulnerabilities

Summary

One of the most notable attacks this quarter has been the SQL Injection which has affected hundreds of thousands of servers. At the beginning of April it was detected that numerous servers had been compromised. Their web pages had been modified to include an iframe pointing to a server which exploited several vulnerabilities: MS06-014, MS07-004, MS07-018, MS07-033, MS07-055... These vulnerabilities were exploited to distribute different strains of malware.

Initially, it was thought that there was a zero-day exploit in Microsoft's IIS or SQL Server. However, Microsoft denied the existence of any vulnerability in its products. In fact, it was a case of well organized SQL Injection attacks. Given the number of servers affected, the attack must have been automated, using a tool designed specifically to scan servers, analyzing the possibilities for SQL injection in each server. This attack once again demonstrates the potential financial benefits from IT attacks and malware distribution, as the malware distributed in this case was designed for stealing bank details.

On the other hand, Microsoft has finally published Service Pack 3 for Windows XP. This is a collection of the patches published since the last Service Pack. It is advisable to install this service pack to keep your system free from vulnerabilities.

Vulnerabilities that affect Microsoft products (Word, Access, Works, etc.) have been on the rise this quarter. Malware-spreading zero-day vulnerabilities have continued to emerge.

Microsoft Access and its vulnerabilities

In the previous quarterly report we mentioned the growing number of vulnerabilities affecting MDB files, and how Microsoft refuses to publish patches as it considers this file format to be highly unsafe.

Finally, after techniques for how to exploit certain vulnerabilities in Access using Word files became public, Microsoft published the patches needed to resolve these problems in Access.

Vulnerabilities

Flash vulnerabilities: a growing problem

Vulnerabilities affecting Adobe Flash continue to appear. These are truly critical vulnerabilities as they allow codes to be run on systems simply by visiting a malicious web page with flash code that allows the vulnerability to be exploited. PandaLabs advises users to make sure these applications are kept completely up-to-date, as they have become a highly effective channel for compromising computers.

Banker Trojans

Banker malware (designed to steal online banking passwords, account numbers, etc.) represents one of the most dangerous IT threats in circulation and its rapid expansion – a 400% increase in 2007- is jeopardizing users' security.

This type of malware is causing serious losses for users around the world, particularly considering the increased use of online banking services. In 2006, in the USA alone, there were already 44 million online bank users. This is a tremendous pool of potential victims for cyber-crooks. According to the Anti-Phishing Working Group, in 2006, the average amount stolen from each victim of online fraud was €6,383. Extrapolate this average value to a volume of 7 million clients... and the figure is frightening: €44,681 million.

For this reason, at PandaLabs we have been closely monitoring the evolution of this type of malware.

According to data compiled at the laboratory, Sinowal, Banbra and Bancos are the three most active banker Trojan families. Other families, including Dumador, SpyForms, Bandiv, PowerGrabber and Bankpatch also have numerous variants, while there has been less activity in the Briz, Snatch and Nuklus families of banker Trojans.

Most active families

Among the most active groups of banker Trojans, there have been three main types:

1. Brazilian banker Trojans (Banbra, Bancos)

These are designed principally for stealing passwords to Brazilian and Portuguese banks, although the Bancos family also targets Spanish banks occasionally. They normally transmit the information obtained through FTP or email.

The difference between the families lies in the programming language. Banbra uses Delphi, while Bancos is programmed in Visual Basic.

Unlike other families, they are not created with Trojan generator kits but are programmed individually.

Banker Trojans

2. Russian banker Trojans 1.0 (Cimuz, Goldun...)

There are many variants of these families, as they are often designed using Trojan creation kits. However these tools have not changed in recent years, and so cyber-crooks are creating new variants, but with the same Trojan kits. One consequence of this is that the variants of both these families of Trojans do not contain new functions, making them relatively simple to detect with antivirus solutions.

3. Russian banker Trojans 2.0 (Sinowal, Torpig, Bankolimb)

Currently these are the most active families, and as they are continually changing and being updated (targeting new banks), they are also the most dangerous. This makes it difficult for antiviruses to detect them generically.

All of them have one common function: the list of target banks and organizations is obtained from a configuration file, so the Trojan itself does not need to be modified in order to add a new target bank. They also use stealth and polymorphic techniques to make detection more difficult.

The following graph shows the number of detection of variants of various families since 2008:

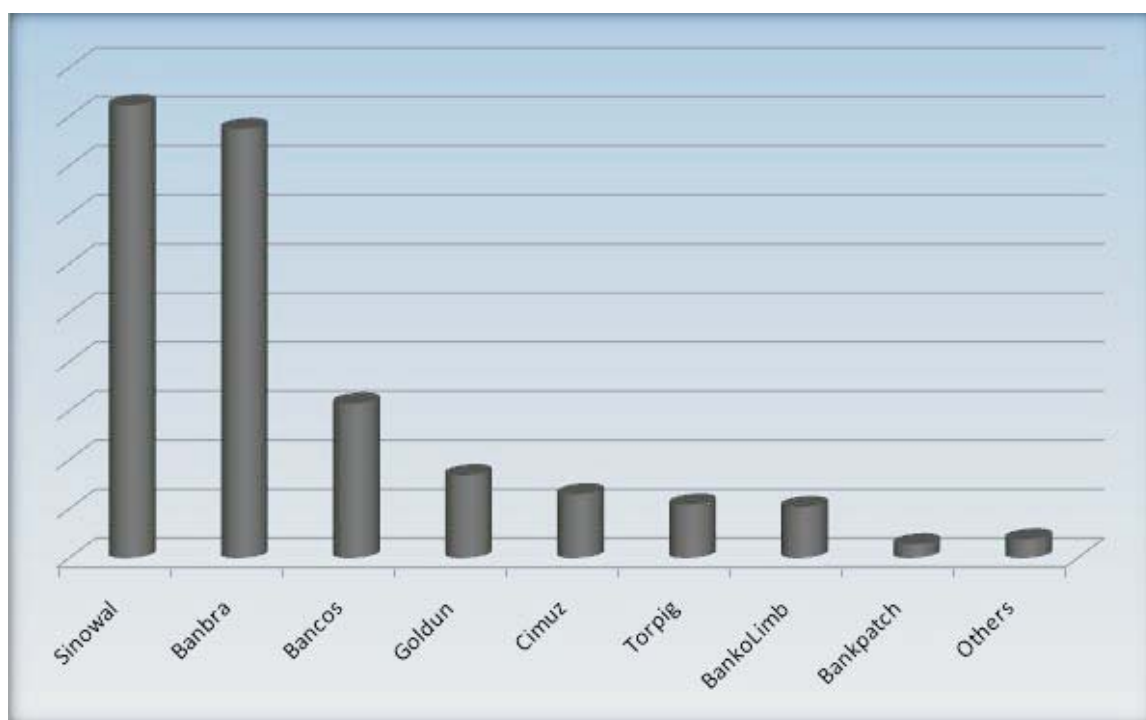


Figure 10. Samples detected since January 2008

Banker Trojans

Trends and conclusions

This analysis indicates which families are most active, although this doesn't mean that less active families are any less dangerous. Some of them, such as Briz and Snatch, have caused numerous problems in the past and could do so again. For this reason, in addition to the quantitative analysis it is advisable to analyze these infections qualitatively.

The Torpig family, one of the most active, now includes rootkit functions. It is no ordinary rootkit, this is one of the most innovative that we have seen so far, modifying the Master Boot Record or MBR and loading itself from there. This makes it very difficult for it to be detected by a security solution and more complex still for infected users to recover their system.

Variants of the Sinowal Trojan have also been modified with similar aims – to impede detection. The malicious codes in this family vary the file that they generate and continually modify their packer, making generic detections more difficult. The Bankolimb family, on the other hand, has altered their data encryption method.

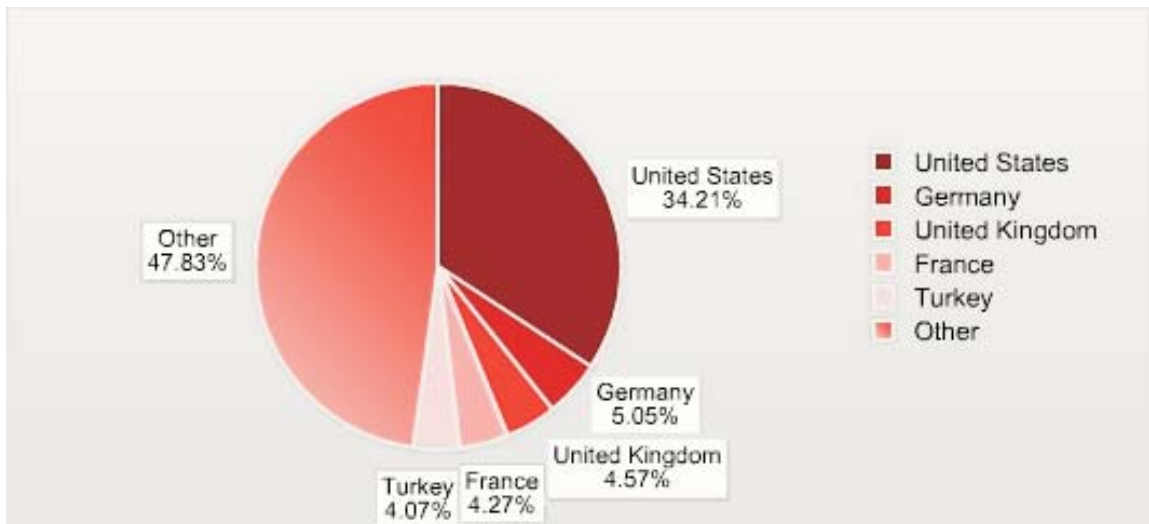
One observation we have made recently is that there are hardly any new families emerging. There are simply new and improved versions of existing families. Such improvements include new functions, the use of packers with different encryption methods, or rootkit techniques to prevent being detected.

Spam and Phishing situation

Spam status in Q2

During the first months of 2008, spam levels fluctuated between 60 and 94 percent of all email sent across the Internet.

The current TOP 5 spam producing countries are:



Source: [Commtouch Software Online Labs](#)

Figure 11. Top 5 spam producing countries

Botnets are still the most widely used method for distributing spam. They are rented or sold to the highest bidder, and are becoming more effective with the increased amount of broadband connections available.

The figures below describe the distribution of zombie computers by country:

Turkey	10.4483%
Brazil	8.7601%
Italy	7.1383%
Russian Federation	6.8582%
Germany	5.8042%
Poland	5.5778%
India	5.0865%
United States	4.7575%
Spain	4.2397%
Colombia	3.8093%

Spam and Phishing situation

Distribution of spam on social networks

One of the most interesting details about spam distribution in this second quarter has been the use of social networks. This is not the first time we have observed this, at the beginning of the year we noted how spam was being distributed in images hosted on the Flickr network. This time however, spam has reached Twitter.

● Twitter	You are followahottie19's newest friend!	Today	6:05 AM
● Twitter	You are videos's newest friend!	Today	5:21 AM
● Twitter	You are virtual worlds's newest friend!	Today	5:20 AM
● Twitter	You are Internet News's newest friend!	Today	5:19 AM
● Twitter	You are gadgets's newest friend!	Today	5:18 AM
● Twitter	You are singers sing music's newest friend!	Today	5:18 AM
● Twitter	You are robots's newest friend!	Today	5:17 AM
● Twitter	You are Education's newest friend!	Today	5:16 AM
● Twitter	You are Bird Flu's newest friend!	Today	5:15 AM
● Twitter	You are tracylords's newest friend!	Today	5:04 AM
● Twitter	You are JunkDNA Fiction's newest friend!	Today	3:46 AM

Figure 12. Spam in Twitter

Twitter users are receiving waves of emails through the Twitter internal system, informing of the existence of new followers. So far nothing unusual. However, these new 'followers' only contain advertising in their profiles, which users will see when they try to find out about their new follower.

Will Debt Consolidation Hurt My Credit?. Have you ever wondered.
<http://ucanreach.com/succes...>
 cerca de 1 minuto ago from web

Non Profit Debt Consolidation Vs For Profit Debt Consolidation: Which Is More Cost-Effective?... <http://ucanreach.com/succes...> 05:46 AM April 24, 2008 from web

Pros and Cons of Debt Consolidation. To consolidate or not to — is. <http://ucanreach.com/succes...> 05:46 AM April 24, 2008 from web

Things You Need To Know Before You Consolidate Debt Loans.. <http://ucanreach.com/succes...> 05:45 AM April 24, 2008 from web

How To Make Money Online Blogging - For Beginners. We. <http://ucanreach.com/succes...> 05:45 AM April 24, 2008 from web

A Comprehensive Review of Filling Medical School Applications.. <http://ucanreach.com/succes...> 05:45 AM April 24, 2008 from web

How Can A Montessori School Save You Money?. 147e Is it to a. <http://ucanreach.com/succes...> 05:45 AM April 24, 2008 from web

Figure 13. Spam in Twitter

Spam and Phishing situation

This brings us to the question: Is there actually any point in this type of spam on Twitter? Well there probably is, as even though users know it is spam, and they reject these spammer followers, the advertising content is still viewed by numerous users.

Phishing Kits / Fake Pages

Every day, most of us receive countless junk emails, otherwise known as [spam](#). Nevertheless, what possible motive can there be for sending so much spam if nobody pays any attention? Perhaps we are wrong. Perhaps people do pay attention.

Some of these messages use highly credible social engineering techniques leading some users to read the spam, click on a link, or open attachments.

One of the reasons for the increase in spam is that it is still highly profitable.

It has also evolved considerably since the phenomenon first appeared, not just in techniques for evading spam filters but also in the content of the messages. While many of them offer pharmaceuticals, watches, electronic gadgets, etc...and are clearly identifiable as spam, others use basically similar techniques or tools to distribute [phishing](#) emails, scams, hoaxes, etc...

Phishing or Fake Page attacks targeting any online service can be easily launched without any significant outlay, and are therefore potentially highly profitable.

Spam and Phishing situation



Figure 14. Fake Page



Figure 15. Folders of social networks

Spam and Phishing situation

<u>Name</u>	<u>Last modified</u>	<u>Size</u>
 Parent Directory	06-Apr-2008 08:31	-
 letters/	06-Apr-2008 08:34	-
 militarybankonline.b..>	06-Apr-2008 05:54	116k
 online.anz.com.au.zip	06-Apr-2008 06:33	48k
 online.wamu.com.zip	06-Apr-2008 06:51	8k
 online.westpac.com.a..>	06-Apr-2008 06:42	37k
 www.bankofamerica.co..>	06-Apr-2008 06:56	41k
 www.cahoot.com.zip	06-Apr-2008 08:35	85k
 www.chase.com.zip	06-Apr-2008 05:57	77k
 www.e-gold.com.zip	06-Apr-2008 05:58	66k
 www.e-trade.com.zip	06-Apr-2008 05:59	126k
 www.ebay.com.zip	06-Apr-2008 05:58	88k
 www.epassporte.com.zip	06-Apr-2008 05:58	301k
 www.hsbc.co.uk.zip	06-Apr-2008 06:00	348k
 www.lloydstsb.com.zip	06-Apr-2008 06:00	45k
 www.moneybookers.com..>	06-Apr-2008 06:01	331k
 www.nationwide.zip	06-Apr-2008 06:34	13k
 www.natwest.com.zip	06-Apr-2008 06:48	18k
 www.paypal.com (200..>	07-Apr-2008 15:43	388k
 www.paypal.com.zip	06-Apr-2008 06:01	212k
 www.sunnbnj.com.zip	06-Apr-2008 06:02	256k
 www.tdcanadatrust.zip	06-Apr-2008 06:36	25k
 www.usbank.com.zip	06-Apr-2008 06:04	98k
 www.wachovia.com.zip	06-Apr-2008 06:05	73k
 www.wellsfargo.com.zip	06-Apr-2008 06:45	180k
 www.westernunion.com..>	06-Apr-2008 06:06	111k

Figure 16. Folders of fake pages

Spam and Phishing situation

One of the undisputed advantages of the Internet is the ease with which useful information can be obtained, and as with many things, the use applied to such information is up to the individual. In the case at hand, it is easy for any Internet user to find information on how to launch phishing attacks. There are blogs, forums and videos offering clear instructions for beginners.

A phishing kit targeting a specific service “which is no more than a series of files that contain a fake web page”, a site to host the fake page, a mail list, and a mailer inbox or tool for sending email, are four of the basic tools required for phishing.

Phishing attacks are generally related with fraudulent online banking web pages, yet there are many other online services targeted by the underground community, with the corresponding phishing kits and fake pages.

The modus operandi is similar to that of phishing targeting banking services. Using mass-mailing tools, the fake message is sent to numerous addresses. The message includes a link, supposedly to the online service in question, but the real URL is that of the spoof web page.

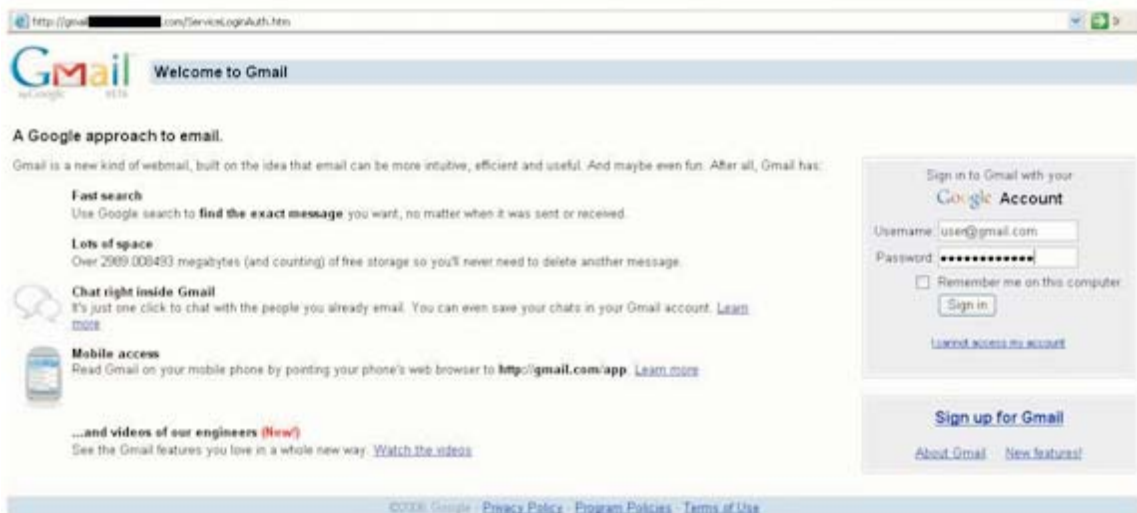


Figure 17. Google fake page.

Spam and Phishing situation

If users do not realize that the page is fraudulent, they could enter their login details. This information is then stored in a file which the cyber-crook can collect later. Sometimes the information is sent to an email address belonging to the creator of the kit.



Figure 18. Google credentials.

There are other peripheral businesses related to phishing and scams. For example, people who compile lists of email addresses and sell them to the highest bidder (sometimes organized by age, country, or domain), spammers who rent out their infrastructure for mass-mailing, people who specialize in recruiting 'mules', etc.

Yet even though this market exists, it is still possible to set up a phishing operation without spending a cent. It is easy nowadays to find places to host web pages. The fake pages and emails, as you can see above, can also be obtained with a bit of diligent searching on the Internet. Mass-mailing lists can be acquired through applications designed specifically for this purpose, although without any great effort, it is possible to collect as many as 20 million addresses on P2P networks.

Even supposing that the success rate of the spam was as low as 1%, this would mean 200,000 recipients accessing the false Web page, and therefore it is easy to see the scale of the potential financial returns.

Perhaps that's why these annoying emails still saturate our inboxes, as relative novices in the world of cyber-crime are lured into the professional ranks by such tempting potential returns.

Spam and Phishing situation

Below you will see some screenshots of these kits; note the accuracy of the false web pages in particular.

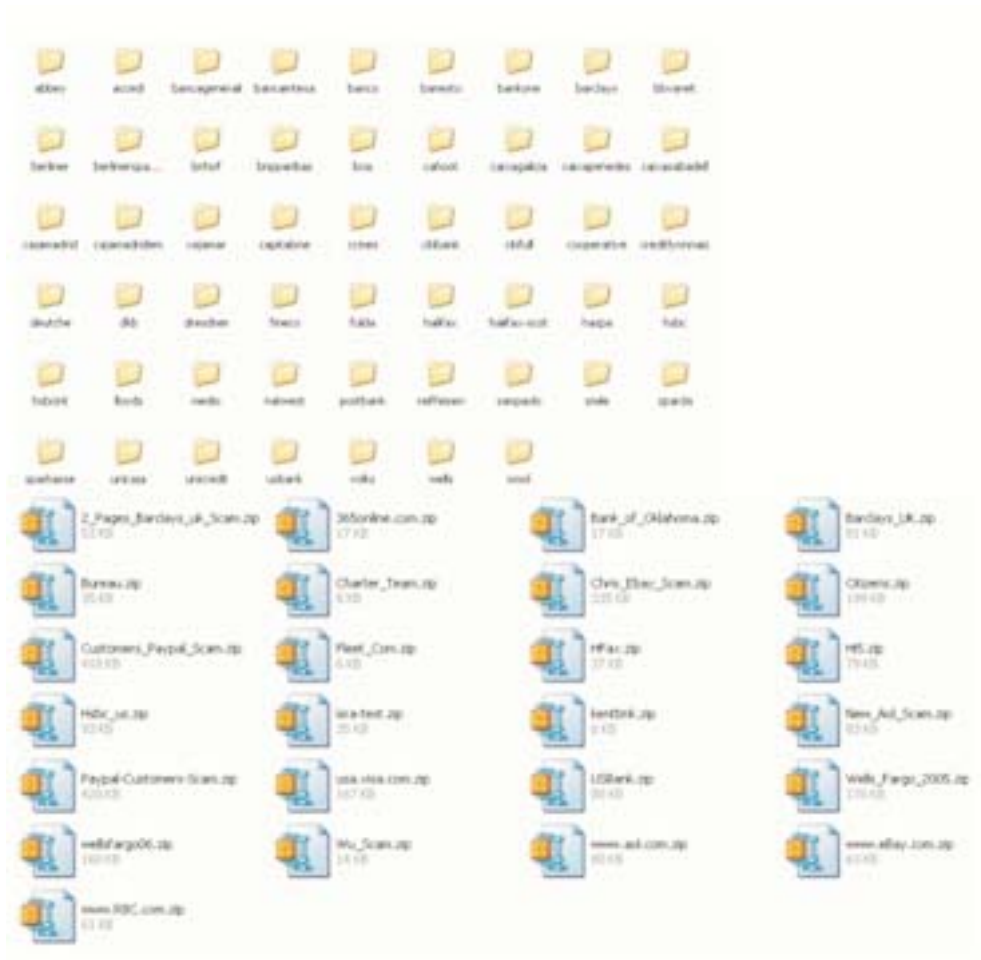


Figure 19. Phishing kits

Spam and Phishing situation



Figure 20. Fake page of bank 1

An example of a fake email and web page targeting a bank.



Figure 21. Fake page of bank 2

Spam and Phishing situation

As mentioned, it is not only banks that are targeted, there are kits targeting services such as Yahoo, Hotmail, Gmail, Youtube, Xbox, Fotolog, etc. In fact, it would seem that any online service is a potential target for the theft of login details, etc.



Figure 22. Xbox page



Figure 23. Advertisement in a forum

Spam and Phishing situation

Some kits include a tool for sending fake pages via email, so anyone can use them without understanding HTML, PHP, or other programming languages.

The screenshot shows a web interface for a tool named "Rzor mailer". It features several input fields and controls:

- tu correo:** Input field for the sender's email address.
- tu nombre:** Input field for the sender's name.
- devolver a:** Input field for the return email address.
- adjuntar archivo:** Input field for an attachment, with an "Examinar..." button next to it.
- tema:** Input field for the email subject.
- mensaje :** A large text area for the email body.
- Email objetivo / Email enviar a :** A text area for the recipient's email address.
- Formato:** Radio buttons for "Plain" (selected) and "HTML".
- numero a enviar:** Input field with the value "1".
- maximo tiempo de ejecucion del script(en segundos, 0 para limite):** Input field with the value "0".
- enviar correos:** A button to send the emails.

Figure 24. Tool for sending fake pages via email

Given the easy access to these kinds of tools, it is easy to understand how malicious users are profiting from them. This lucrative business model will no doubt lead to more fake pages for online services being created and more spam reaching our inboxes.

About PandaLabs

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

- **PandaLabs** creates continually and in real-time the counter-measures necessary to protect Panda Security clients from all kind of malicious code on a global level.
- **PandaLabs** is in this way responsible for carrying out detailed scans of all kinds of malware, with the aim of improving the protection offered to Panda Security clients, as well as keeping the general public informed.
- Likewise, **PandaLabs** maintains a constant state of vigilance, closely observing the various trends and developments taking place in the field of malware and security. Its aim is to warn and provide alerts on imminent dangers and threats, as well as to forecast future events.
- For further information about the last threats discovered, consult the **PandaLabs** at: <http://pandalabs.pandasecurity.com/>.