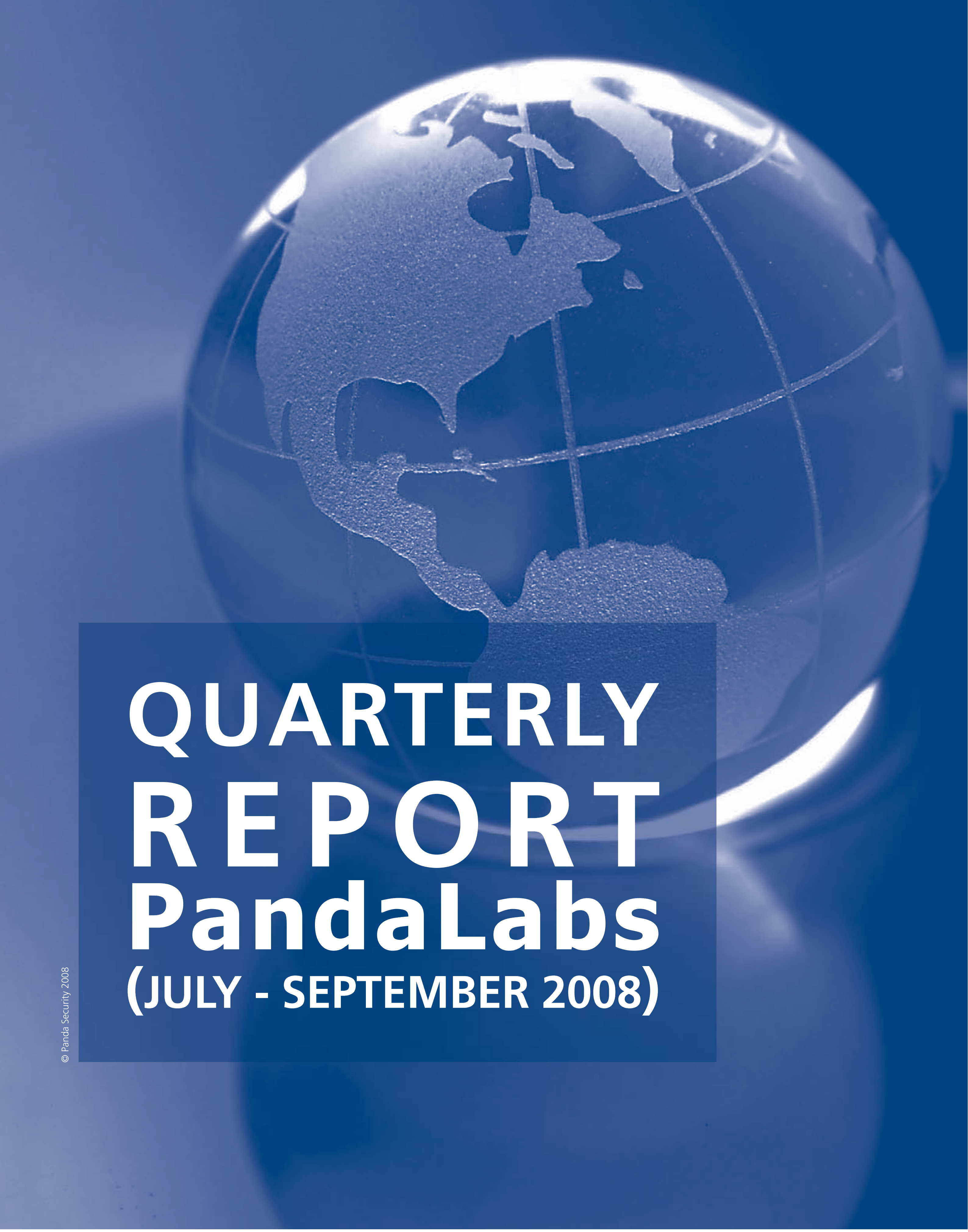


QUARTERLY REPORT PandaLabs

(JULY - SEPTEMBER 2008)

One step ahead.

www.pandasecurity.com

Index

Introduction

As Q4 begins, it is time we looked back at Q3. You might think that the third quarter of the year would be the calmest, as it's when most countries in the northern hemisphere have summer vacation periods. Cyber-crooks, however, don't take summer breaks.

A serious DNS server vulnerability was detected, leading to a massive coordinated patching of DNS servers. For further information, check out the vulnerabilities section.

Collective intelligence is an innovative technology which will be on everyone's lips from now on, and is integrated in our new 2009 products. We have prepared an article to give an insight into this innovative concept.

Spam is still an issue, regardless of all efforts made to deal with it, cyber-crooks come up with new ways of saturating users' mailboxes with unwanted mails.

Social networks are all the rage and cyber-crooks know it. We will talk about their popularity and the main attacks they have suffered in the last few months.

As in previous reports, we will present the evolution of active malware by country throughout the year so far, and the Q3 malware figures.

We hope you find it interesting.

Executive summary

According to a research study carried out by Panda Security, clients of ALL antiviruses (Panda included) are infected. The infection rates ranges between 12-13% to 30% approximately.

Adware has gone from 22.03% in Q2, to 37.49% in Q3 due to the amount of fake antivirus programs.

Spain and the U.S. are the countries with the highest active malware percentage in Q3, exceeding 30%.

The US Justice Department reported it would charge 11 people with stealing and selling over 100 million credit and debit cards. The charges include conspiracy, computer intrusion, fraud and identity theft.

A DNS server vulnerability has been detected, which allowed hackers to redirect web pages and domains to a hacker-controlled system.

Third 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 third quarter of 2008:

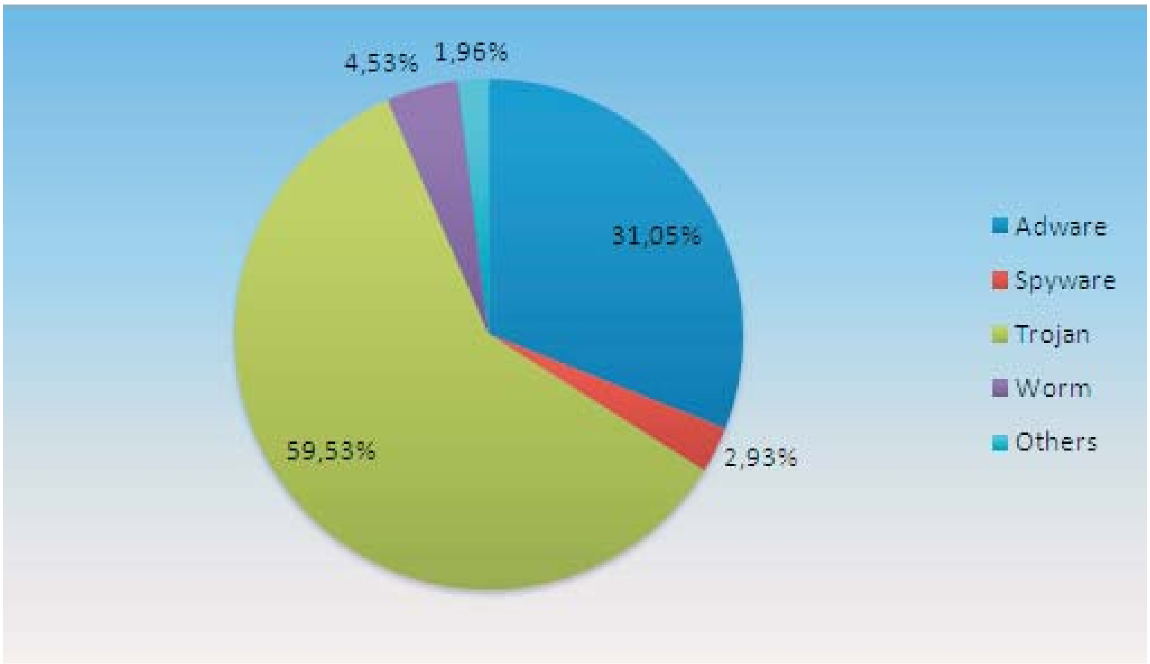


Figure 1. Malware detected inQ3.

Trojans are still the malware most frequently detected by PandaLabs.

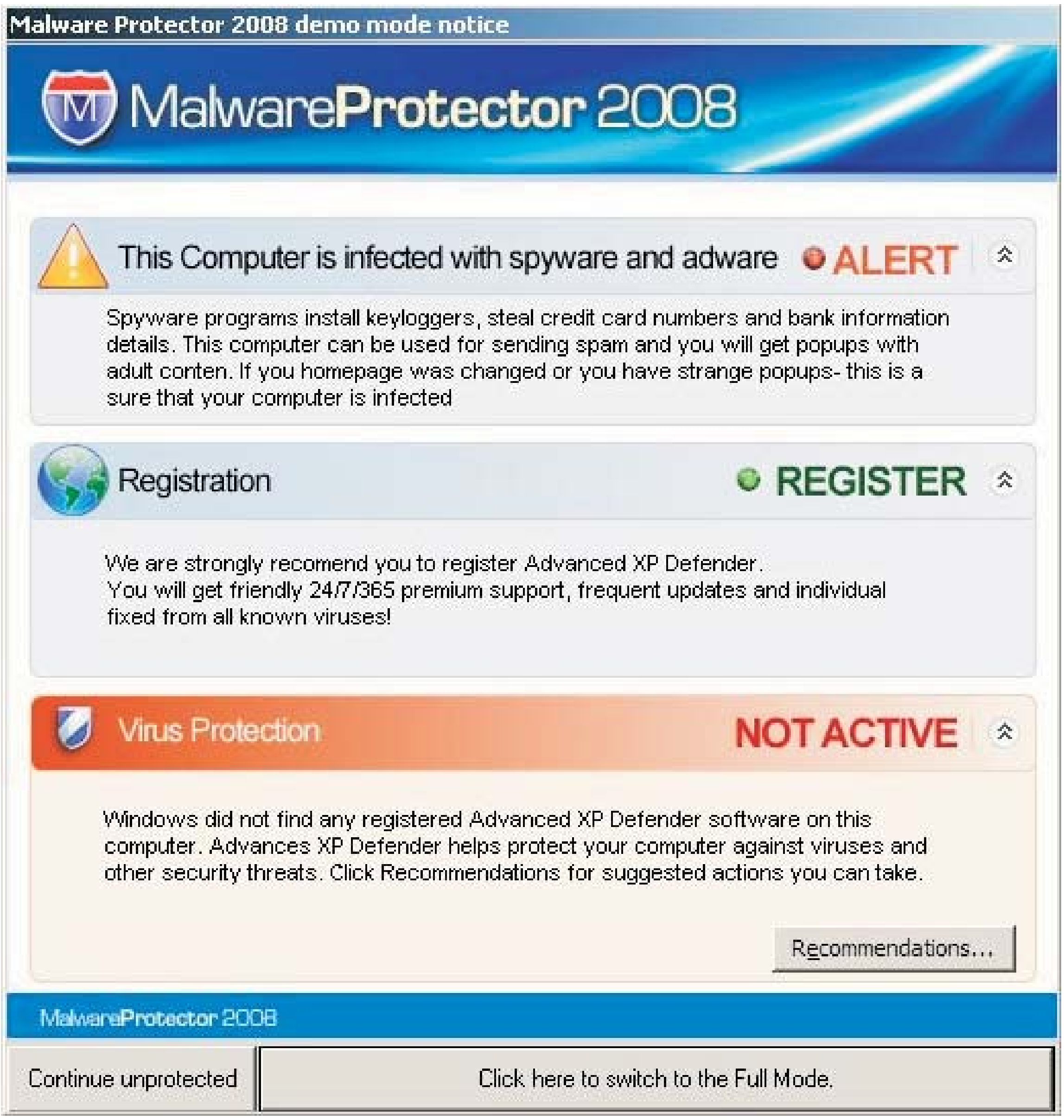
Adware has risen from 22.40% in Q2, to 31.05% in Q3.

This increase is mainly due to the amount of fake antivirus programs detected over this quarter.

Fake antivirus programs are a set of applications that falsely report a computer infection and offer users the possibility of downloading software to eradicate the infection. Once the application is downloaded, users are asked to pay a fee to register and eliminate the infection.

Third Quarter Figures

Below is an example of a fake antivirus program:



Malware Protector 2008 demo mode notice

MalwareProtector 2008

This Computer is infected with spyware and adware ● ALERT

Spyware programs install keyloggers, steal credit card numbers and bank information details. This computer can be used for sending spam and you will get popups with adult conten. If you homepage was changed or you have strange popups- this is a sure that your computer is infected

Registration ● REGISTER

We are strongly recomend you to register Advanced XP Defender.
You will get friendly 24/7/365 premium support, frequent updates and individual fixed from all known viruses!

Virus Protection NOT ACTIVE

Windows did not find any registered Advanced XP Defender software on this computer. Advances XP Defender helps protect your computer against viruses and other security threats. Click Recommendations for suggested actions you can take.

Figure 2. Interface of a fake antivirus program.

Third Quarter Figures

This increase is due to the large amount of spam messages created to distribute this type of program. Additionally, these messages use social engineering techniques to fool users. They also contain malicious links supposedly redirecting to videos related to false news stories or videos supposedly containing erotic images of famous people.

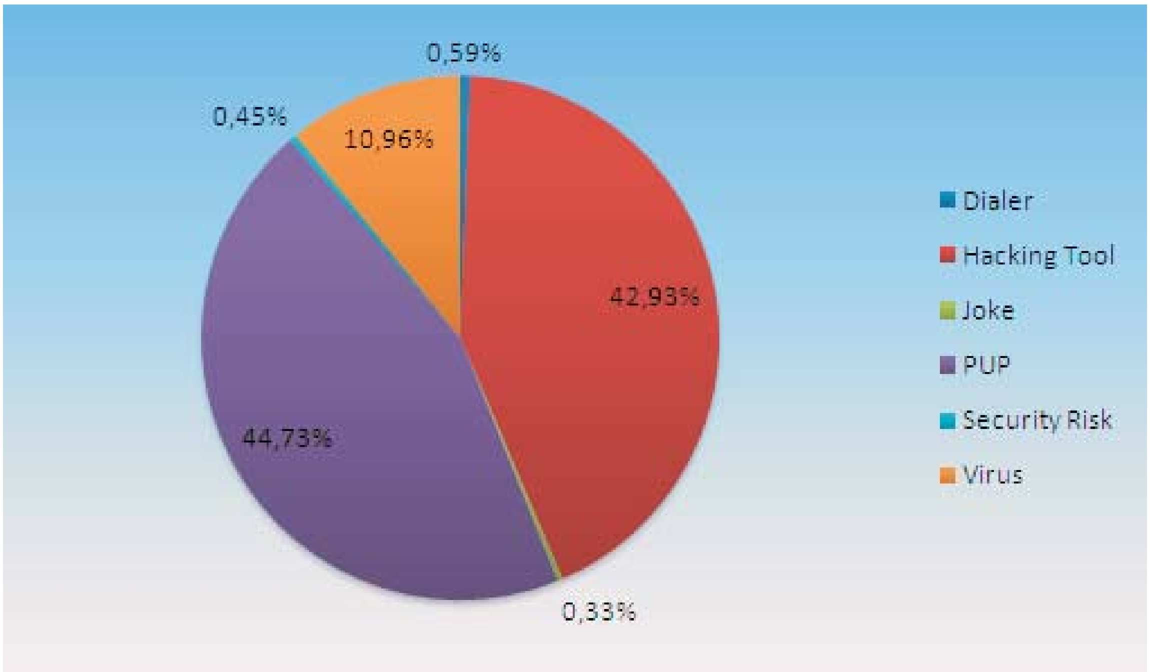


Figure 3. Other malware.

Hacking tools and PUPs (potentially unwanted programs) are the leading malware in this section, at 42.93% and 44.73% respectively.

Third 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.

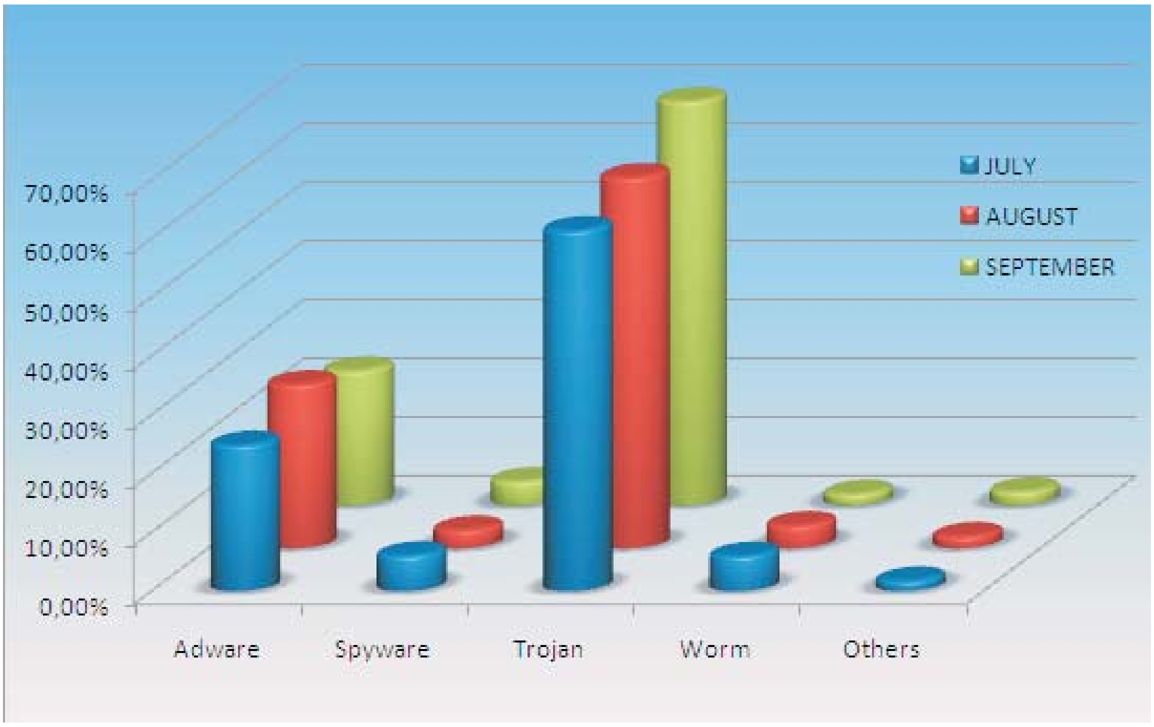


Figure 4. Evolution of the new malware.

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

Third Quarter Figures

Threats detected by the PandaLabs sensors

The following graph shows the distribution of detections made by the PandaLabs sensors throughout the third quarter of 2008.

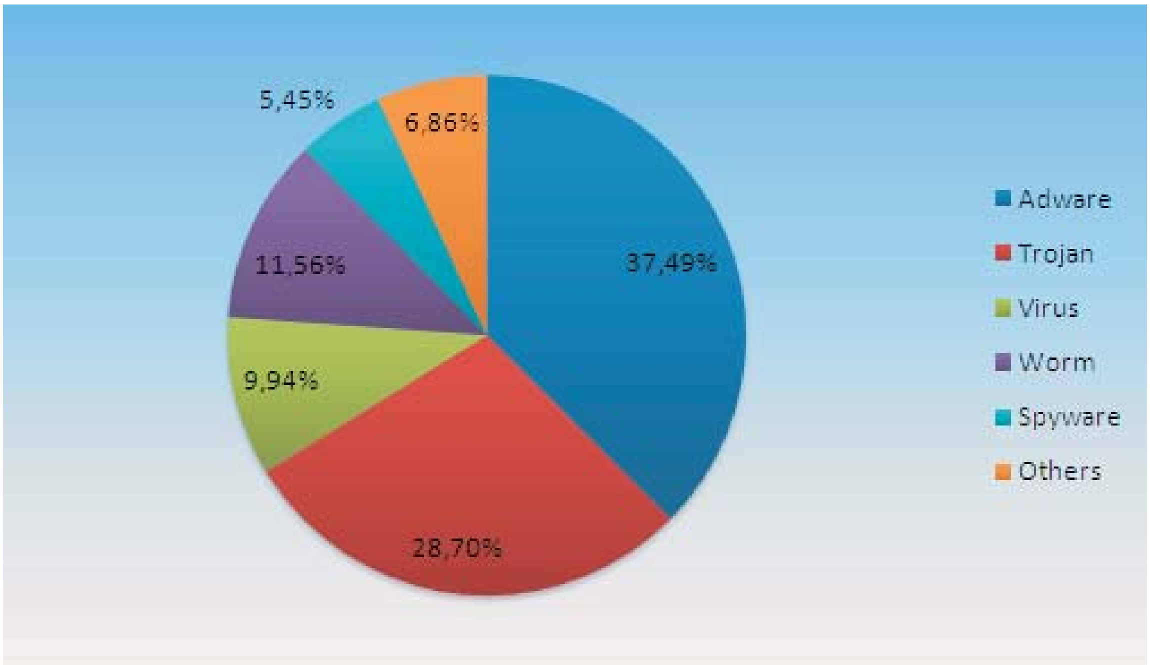


Figure 5. Malware ordered by category.

This graph also shows a significant rise in adware, according to the data gathered by the PandaLabs security sensors.

Adware has gone from 22.03% in Q2, to 37.49% in Q3 due to the amount of fake antivirus programs.

Active malware

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

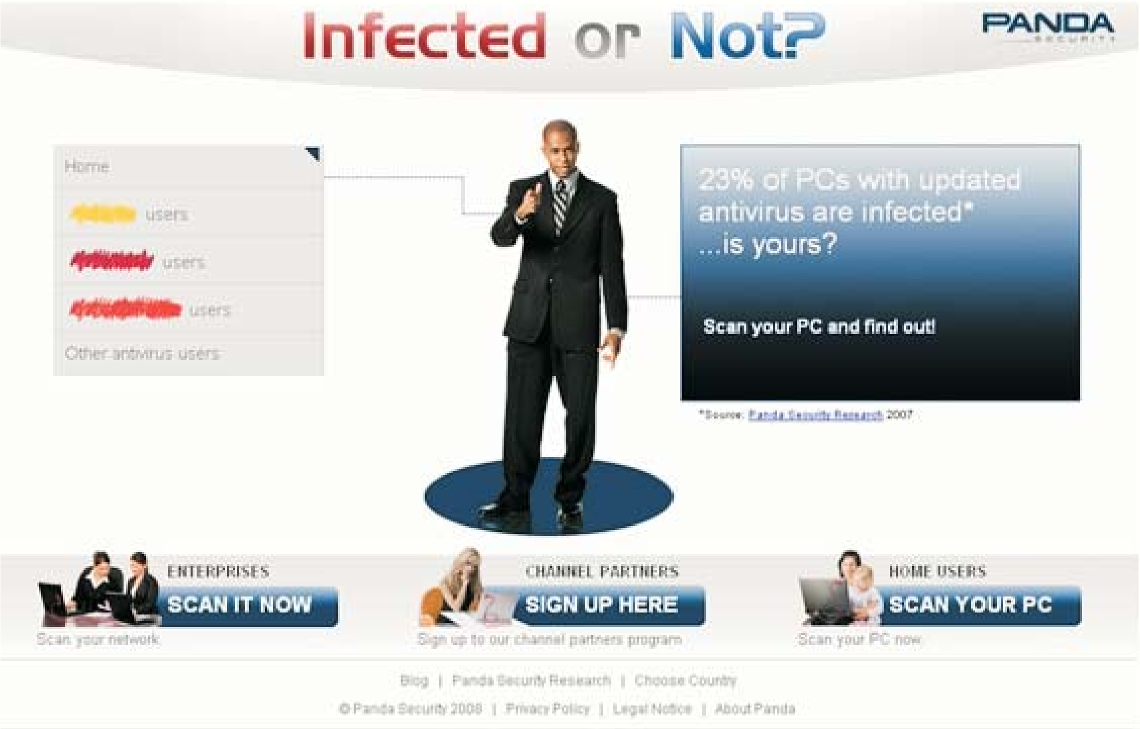
In order to understand what active malware is, we must first define the two possible statuses for malware: active and latent.

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.



Infected or Not?

23% of PCs with updated antivirus are infected* ...is yours?

Scan your PC and find out!

*Source: Panda Security Research 2007

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, but can also consult data for any other country by clicking on it and then on "View statistics". If you want to check the Worlwide infection data just click here.

The graph below shows the evolution of active malware throughout the year so far:

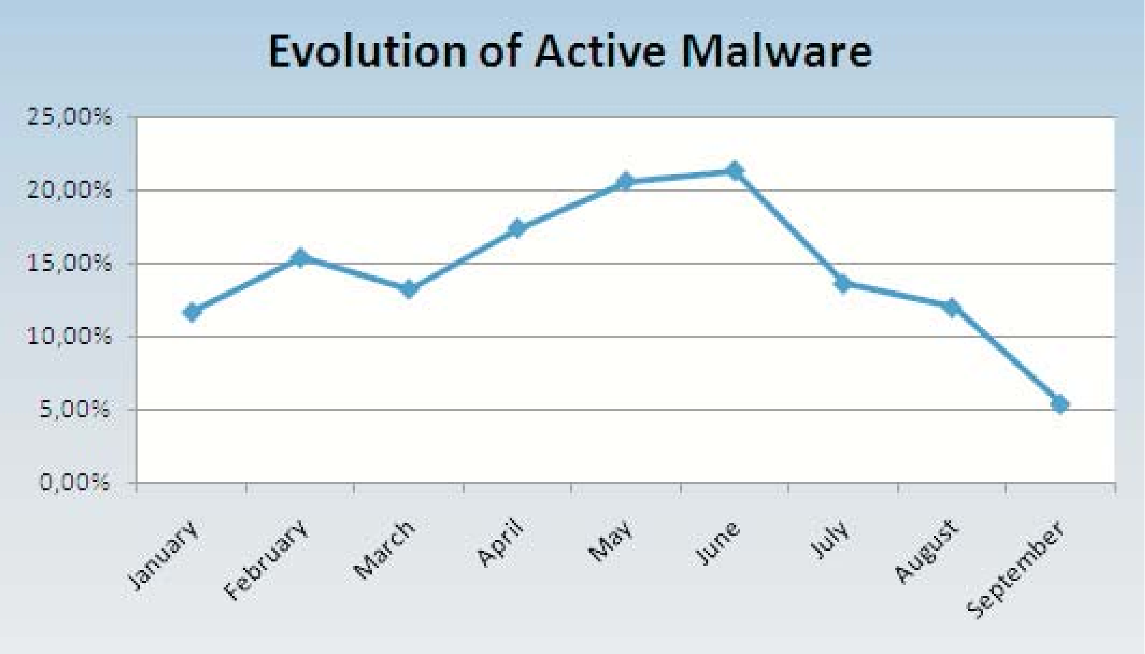


Figure 7. Active malware evolution during 2008.

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 June (21.27%). Since then, the active malware infection rate has progressively decreased, reaching the lowest percentage in September at 5.38%* (*data gathered up to 17/09/2008).

Active malware

At present average active malware reaches 14.48%, almost 3% less than in the first half of the year (17.07%).

This data reflects the evolution globally, but what about in each country? The following graph shows the infection rates of countries with the highest active malware percentage:

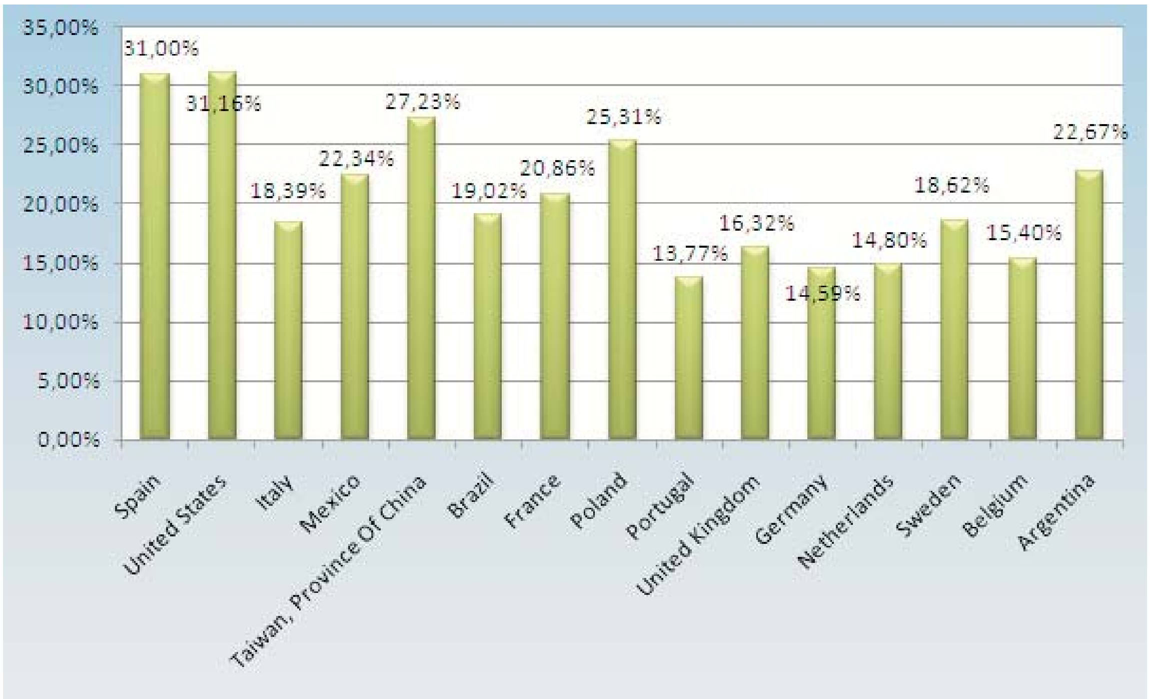


Figure 8. Countries with the highest malware percentage (June-September)[1].

According to the graph, Spain and the U.S. are the countries with the highest active malware percentage in Q3, exceeding 30%.

However, there has been a significant decrease in the number of computers infected with active malware in Q3.

[1] Countries arranged according to the number of analysis carried out.

Active malware

In the first half of the year, all countries exceeded 30% of infection, with Russia, Spain and Mexico exceeding 40%:

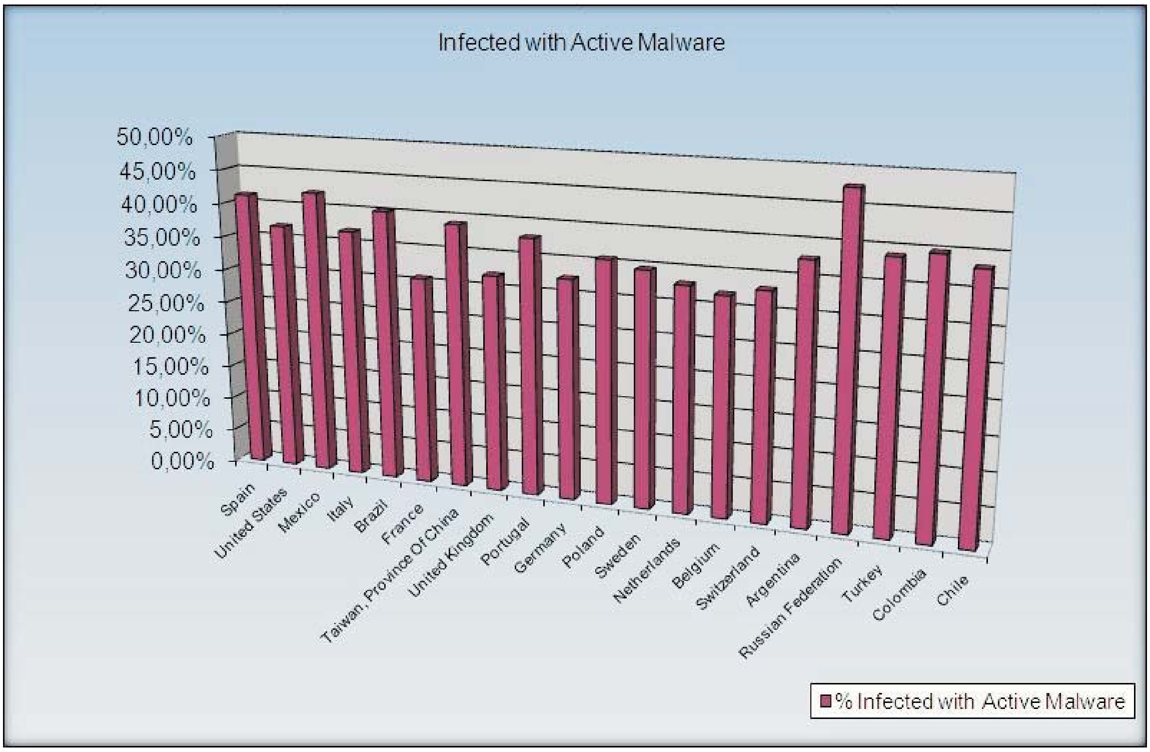


Figure 9. Countries with the highest malware percentage (first half of the year).

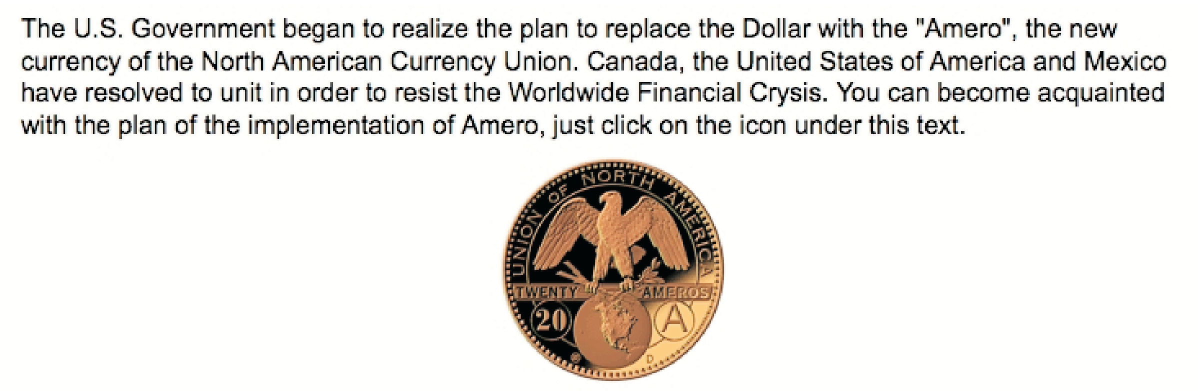
This data is positive, as it shows an improvement in the active malware scenario. Let's hope the downward trend in Q3 is not due to the vacation period, and continues to decrease in Q4.

Q3 trends

You might think that Q3 would be one of the quietest periods of the year, as it coincides with the summer vacation period for many Northern Hemisphere countries. However, the truth is quite the opposite, as the Blaster worm proved in the past. And this year has been no different.

Q3 kicked off with the massive, coordinated patching of DNS servers. This was the first time ever that numerous vendors worked together on this scale to resolve a security flaw. One month later, Dan Kaminsky, the security researcher who reported the vulnerability, outlined the details at the annual Black Hat conference (Las Vegas, USA). He was very clear: "Every network is at risk. That's what this flaw has shown". More technical details, etc. are available in the vulnerabilities section.

Summer storms. Storm worm is still a major issue. In July a message generated by Storm Worm was detected, which once again used social engineering techniques. This time the message informed about the creation of a currency called “Amero” that would replace North American dollars:



The U.S. Government began to realize the plan to replace the Dollar with the "Amero", the new currency of the North American Currency Union. Canada, the United States of America and Mexico have resolved to unit in order to resist the Worldwide Financial Crysis. You can become acquainted with the plan of the implementation of Amero, just click on the icon under this text.

Figure 10. Message generated by Storm Worm.

Regarding cyber-crime, this summer has brought good news. The US Justice Department reported it would charge 11 people with stealing and selling over 100 million credit and debit cards. The charges include conspiracy, computer intrusion, fraud and identity theft.

Q3 trends

The defendants are said to have entered retailers' networks (TJX Cos, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble, Sports Authority, Forever 21 and DSW) through wireless networks. Then hackers installed Trojans that allowed them to capture all kinds of data: credit card numbers, passwords, etc. The data stolen was sent to servers controlled by hackers in the USA and Eastern Europe.

The alleged hackers come from a variety of countries: 3 Americans, 1 Estonian, 3 Ukrainian, 2 Chinese and another accused whose nationality is still unknown.

DNS vulnerability

This quarter we must highlight the detection of the DNS server vulnerability which allowed hackers to redirect web pages and domains to a hacker-controlled system.

The DNS protocol is a system that translates web page names into IP addresses the Internet can interpret. E.g. the www.pandasecurity.com web page is translated numerically as 88.221.26.28. When users access a web page, the Internet interprets the numbers associated to that page.

The researcher Dan Kaminsky discovered this vulnerability after months of investigation. He was due give a full description of the vulnerability in the Las Vegas Black Hat event at the beginning of August. However, the information was published on a famous blog by error, and was accessible even after being deleted from the blog.

The vulnerability uses two famous features of the DNS protocol:

Prediction of source port and transaction ID

DNS uses UDP packets to send and receive requests. Most DNS servers use the same source port to connect to another DNS server in a short period of time. Transaction IDs on the other hand, are random. This security measure is insufficient, and malicious users could create and send false response packets to the attacked DNS server before the authorized DNS server sends a response.

We have included several images to better explain different DNS server situations.

DNS vulnerability

The following image shows an ordinary process in which a user requests access to a specific web page (www.pandasecurity.com in the example):

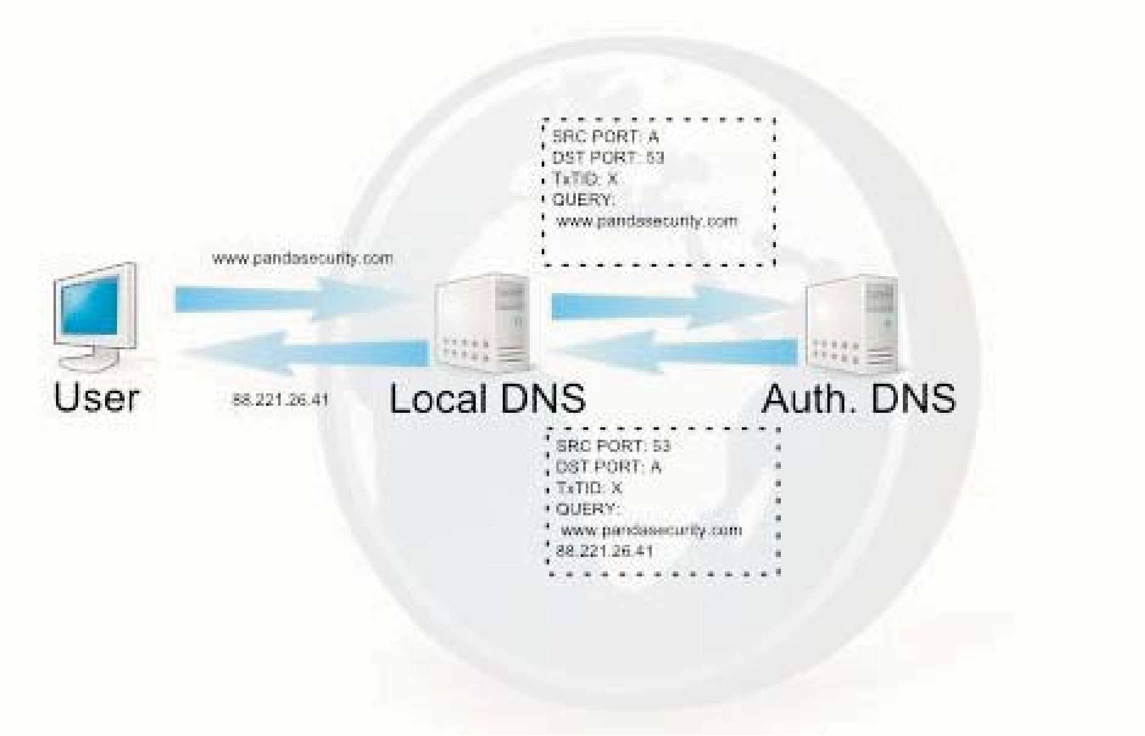


Figure 10. Usual process of a DNS server.

As you can see, there is a source port (A), a target port (53) and a random transaction ID.

DNS vulnerability

In the image below, a malicious user creates a spoof DNS server to find out which port is the source port and use it for malicious means:

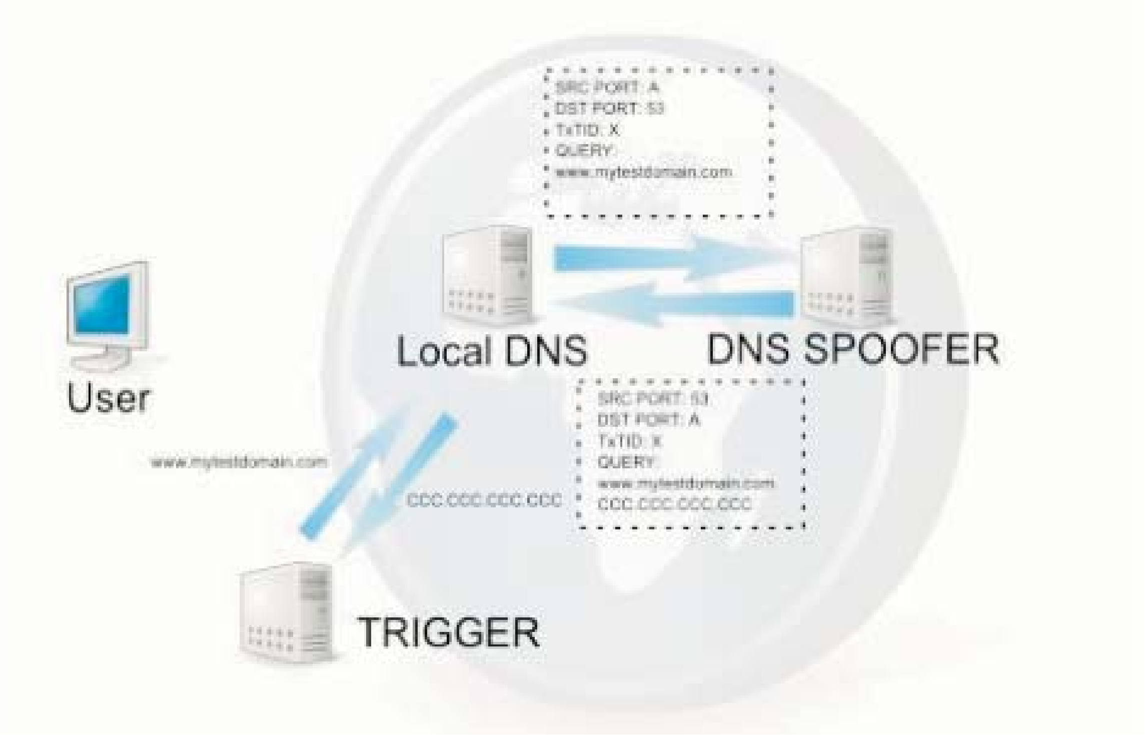


Figure 11. Process with a spoof DNS server.

DNS vulnerability

A trigger is used to find out which source port is used by the Local DNS. In order to do so, the trigger forces the local DNS to send requests to the spoof DNS.

Finally, the image below shows an attack to a DNS server:

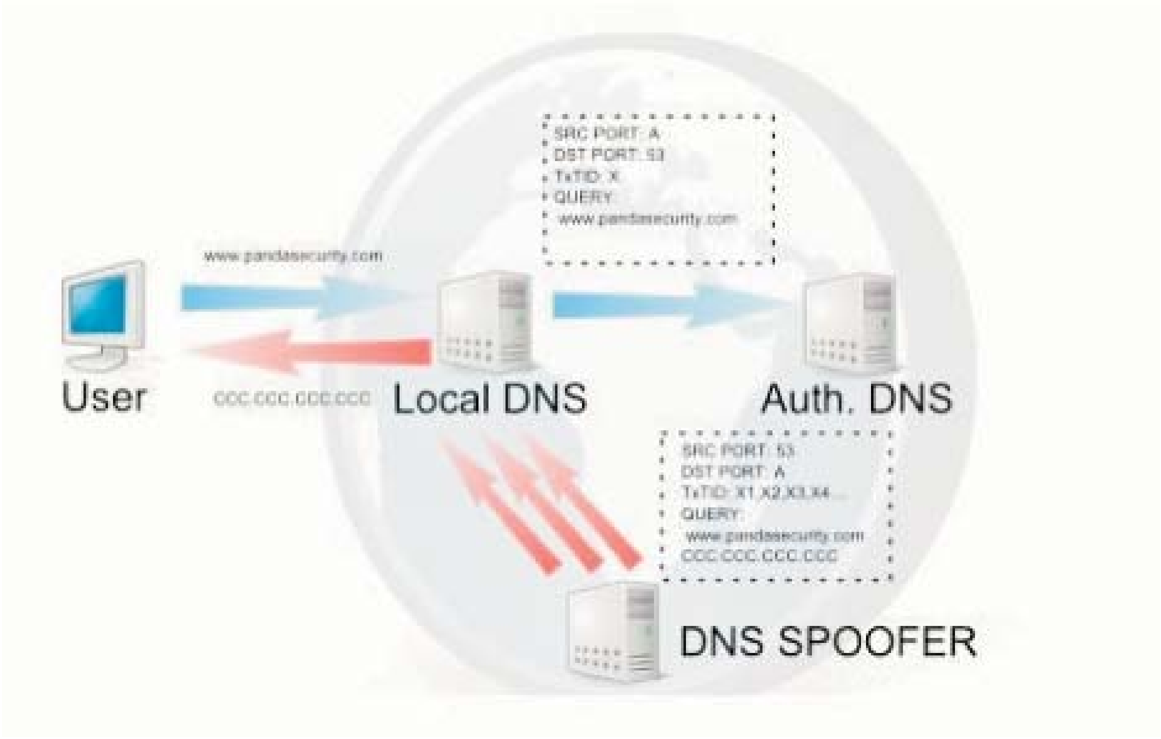


Figure 12. Attack to a DNS server.

Thanks to the spoof server, the attacker can predict the source and target ports. As the transaction ID is random, the spoof DNS server constantly sends packets with different transaction IDs until it finds a valid one. If the packets sent by the DNS spoofer arrive before those of the authorized DNS, the affected user will be redirected to a web page selected by the attacker.

DNS vulnerability

Additional resource registries

DNS servers can include additional information in their response to prevent future questions and improve process efficiency, e.g. the IP address of the attacked domain's server names.

These two features (Prediction of source port and transaction ID and, additional resource registries) would allow attackers to monitor all the traffic sent to the domain.

This is the first time numerous vendors (Cisco, Microsoft, etc.) have worked jointly –and rapidly- to ensure users' security. Regardless of the fact that details of the flaw were leaked early, without this collaboration the consequences would have been much worse. In any case, there is no room for complacency as there are still many systems that have not been patched.

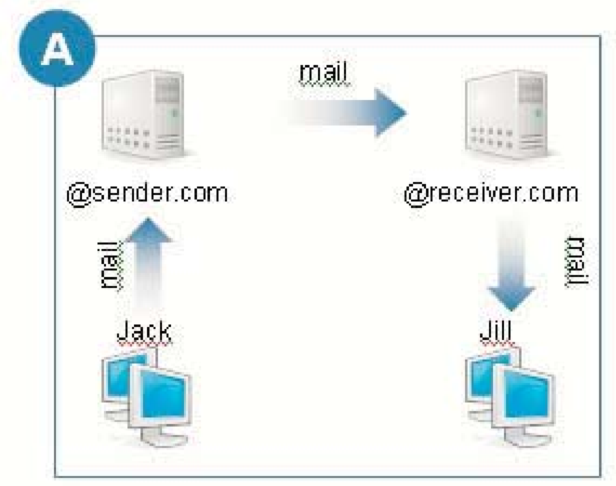
NDRs: the evolution of the sending of spam

The last year has witnessed a notable rise in the number of NDR threats in circulation.

A NDR (Non-Delivery Report) is an automatic mail message from a mail system informing the sender about a delivery problem

NDRs are therefore not spam, but legitimate emails usually delivered by badly-configured mail servers. At present, leading anti-spam companies do not consider that spam is defined by content, instead they regard spam as "unsolicited emails sent on a massive scale". NDRs are regarded as solicited mail, as in theory they respond to an email sent by the victim. Anti-spam techniques used up to the present are therefore not applicable to this type of messages.

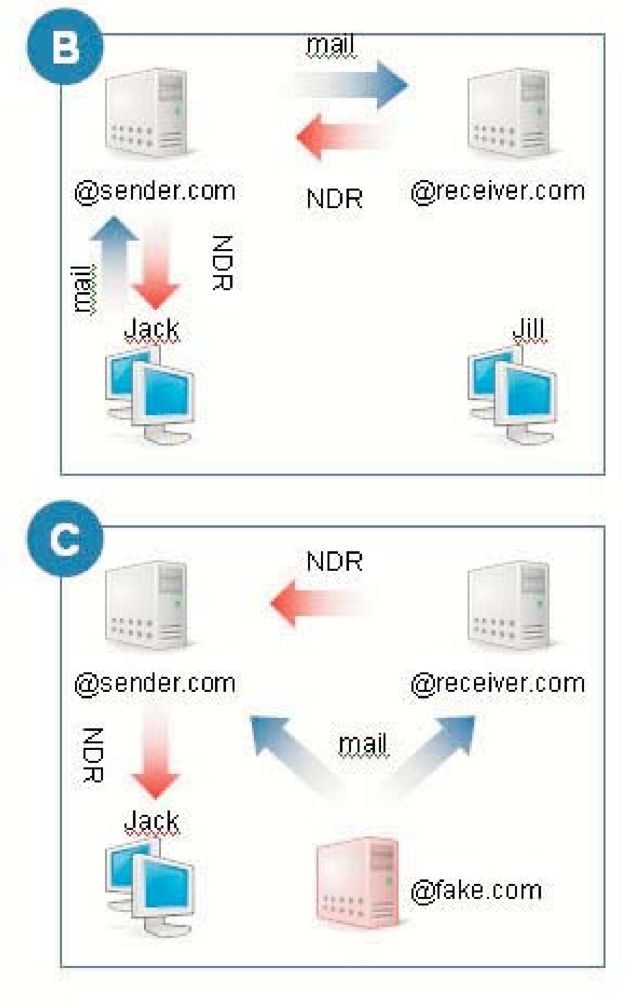
The diagrams below have been included to explain the mail flow. In these examples jack@sender.com wants to send an email to Jill@receiver.com.



In case A, Jack sends a message through his @sender.com server. Jack's server communicates with the @receiver.com server and sends the server the message.

Case A is an example of a successful delivery.

NDRs: the evolution of the sending of spam



In case B, Jack makes a mistake when writing Jill's address. When Jack's server sends the mail to Jill's server (@receiver.com), the server returns a message (NDR) indicating that the address doesn't exist. This message is sent to Jack's server, who in turn places it in his mailbox.

Upon receiving the NDR Jack realizes Jill hasn't received his email because he wrote the wrong address.

Spammers have taken advantage of this service provided by mail systems to fool mail servers and SPAM users (case C). NDRs are also a result of massive emails sent by spammers to automatically-generated addresses.

Legitimate NDRs are therefore generated on sending emails to non-existent addresses pretending to be Jack. This way, when the servers realize the accounts the messages are sent to do not exist, they send an NDR to Jack's account, informing them that the addresses they are trying to email to do not exist.

Jack therefore receives NDRs of messages he hasn't sent (non-legitimate NDRs), which sometimes include an attachment of the spam message that caused the NDR.

NDRs: the evolution of the sending of spam

How can a mail server accept emails from people passing themselves off as you?

The SMTP protocol (previous example) does not allow authentication among all mail servers. This flaw allows sender servers to pass themselves off as the original server corresponding to the domain name. Consequently, hackers take advantage of this flaw for email identity theft.

Can the origin of the message be checked?

At server-level, there are technologies and settings that largely prevent the reception of fake-ID mails:

- Sender Policy Framework: Is an extension to the SMTP which allows authorized computers (identified by their IP address) to send mails to a specific domain. The identification process is carried out by the person in charge of the receiver's domain.

- Reject mails from servers without a reverse DNS registration: checks whether the origin is a dynamic or dialup connection (e.g. RTB/56kb), which do not have an authorized reverse DNS.

At mail-client level, signatures or public keys are used; users use public and private keys to digitally sign a message, making identification unique.

This system is useful for checking senders' ID or encoding data that must only be read by the receiver. These technologies work at client mail level and do not prevent NDR problems.

NDRs: the evolution of the sending of spam

Is it possible to tell the difference between legitimate and non-legitimate NDRs?

One of the problems when detecting non-legitimate NDRs is that although there is an RFC that defines the message structure, messages are so diverse as regards configurations and server-types that it is very difficult to define unique detection policies for these types of messages.

There are three types of NDRs:

1. NDR messages with text informing about the error.
2. NDR messages with text informing about the error and headers of the message that caused the NDR.
3. NDR messages with text informing about the error, plus headers and body of the message that caused the NDR.

Since case 3 includes the content of the spam message that causes the NDR, it can be detected as a non-legitimate NDR using common detection techniques based on content analysis.

Messages described in cases 1 and 2 are the most difficult to detect, since the content of the message that caused the NDR is minimal or non-existent.

Conclusion

Some anti-spam solutions have begun to implement NDR (some legitimate, some not) filtering technologies or a mail label system for identifying legitimate NDRs. Due to the high rate of false positives, it cannot be considered a global solution. Additionally, as we have previously commented, mail servers' lack of homogeneity when creating NDRs renders many of these techniques useless.

Regardless of the efforts made to deal with these types of threats, companies and experts know that the solution to these problems is for vendors, companies and institutions to define basic settings for mail systems that prevent this type of abuse.

Social networks in the spotlight

Social networking sites can be defined as "web-based services that allow individuals to construct a public or semi-public profile within a bounded system, articulate a list of other users with whom they share a connection, and view and traverse their list of connections and those made by others within the system."

We live in an increasingly globalized world in which there are many mechanisms for breaking down geographical boundaries. Our concept of communication has changed and social networks have become a useful tool in this new context of global communication.

Social networks stretch around the globe, connecting millions of people, enabling them to share knowledge, hobbies, advice, concerns…

Although these networks vary widely in terms of subject matter, the basic concept is the same: to provide a channel through which users can communicate.

However, the growing popularity of these sites and the trust they engender among users has attracted the attention of cyber-criminals, who have found in them a new conduit for their fraudulent activities.

This article will analyze the reasons for their popularity, supported by data and statistics, before going on to examine how they have been attacked by the criminal fraternity on the Web.

Popularity of Social Networking Sites

Since social networking sites first appeared, the number of users has grown exponentially. Recent data released by Alexa of the 500 most visited sites on the Internet[2] , reveals that there are seven social networks in the Top 50.

[2] Data from September 5th, 2008 taken from the Web page: http://www.alexa.com/site/ds/top_sites?ts_mode=global&lang=none

Social networks in the spotlight

The first of these is *Facebook*, in fifth place, followed by *Myspace* in seventh position, then *Hi5* and *Orkut* in 16th and 19th place respectively. Positions 32, 38 and 47 were occupied by *Flickr*, *Friendster* and *Skyrock* respectively.

Social network	Position	URL
Facebook	5	www.facebook.com
Myspace	7	www.myspace.com
Hi5	16	www.hi5.com
Orkut	19	www.orkut.com
Flickr	32	www.flickr.com
Friendster	38	www.friendster.com
Skyrock	47	www.skyrock.com

Figure 13. Ranking of social networks.

The Google Trend graph below illustrates the number of searches made by users for a word or phrase corresponding to some of the most widely used networking sites:

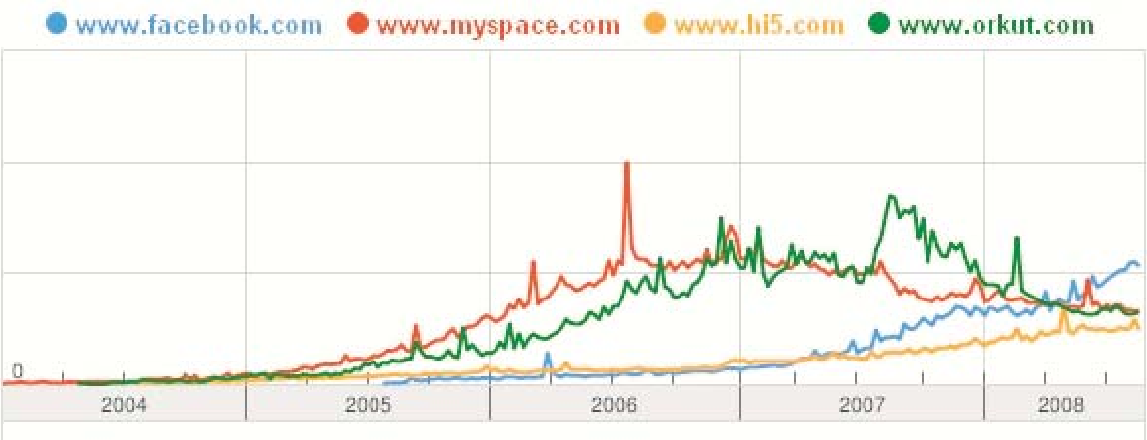


Figure 14. Searches made for the leading social networking sites.

Social networks in the spotlight

The reasons for the success of online social networking are summarized in the following points:

- Human beings are essentially social animals. They need to communicate with others and strive to extend their connections.
- There are no barriers. Social networks break down geographical and even economic barriers that hinder traditional communication.
- Source of knowledge and information. Users of the network share knowledge and data among themselves.
- Online presence. Not everyone is able to have their own Web page. Yet social networks allow individuals to have their own personal page, customized to their own preferences.
- Viral nature. The desire to expand the network of contacts leads users to invite friends, who invite more friends and so on.

Attacks on Social Networks

The popularity of these sites has aroused the interest of cyber-crooks, who have been exploiting them for some years now as a conduit for their fraudulent activities.

The attractions of social networks for the criminally-minded are clear:

- They offer access to countless users, ideal for rapid propagation of malware. If one user is infected, any other user who accesses their infected profile will automatically be infected.
- They store a lot of personal data about people, as in order to use the service users have to create personal profiles. This information can range from names and email addresses to interests, age etc.

  All these details are easily accessed by criminals and can be used for identity theft and targeted attacks or simply sold on to third parties.
- Users of social networks normally trust their contacts. It is not particularly difficult for attackers to steal the identity of a network user and exploit their trusted relationships.

Social networks in the spotlight

Attacks on social networks are not new phenomenon; the first recorded incident occurred in 2005. However, attacks have increased and diversified just as the number of users has grown. These attacks aren't focused exclusively on distributing malware, but also involve phishing, identity theft or propagation of spam.

Notable cases

Most attacks have targeted the most popular social networks such as *MySpace*, *Orkut* or *Facebook*. This doesn't mean that they are any less secure than others, just that they have more users and therefore the chances of the attack being successful are greater.

Below we take a look at some of the most significant attacks on social networks.

MySpace, the most frequently attacked

MySpace, one of the most popular networks, was the first victim and has been attacked on numerous occasions. It was first attacked by a worm created by a MySpace user called MySpace.A, which enabled users to add a million contacts to their list.

At the end of 2006, another worm exploited user profiles to propagate, infecting all users that visited an infected profile.

Around that time, an advertising banner in *MySpace* exploited a Windows Metafile vulnerability to infect over a million users with spyware. Some days later a worm was uncovered at *MySpace* that inserted Java script in user profiles. When somebody tried to visit some of those profiles, they were redirected to a Web page that blamed the U.S. government for the 9-11 attacks.

However, the most serious case took place at the end of 2007. The attackers exploited a feature of Apple's QuickTime player to spread a worm in files that tried to pass themselves off as movies. The film had an HREF track with JavaScript code, allowing hackers to alter the profile of any user that visited the infected profile.

This worm was also designed to send spam massively to all the contacts of infected users. These messages supposedly contained a film. Yet users that tried to see the film would be taken to a pornographic website which downloaded Zango, a type of adware designed to display customized adverts.

Social networks in the spotlight

Security problems in Facebook

Facebook has become one of the most successful social networking sites on the Internet, and consequently, a prime target for criminals.

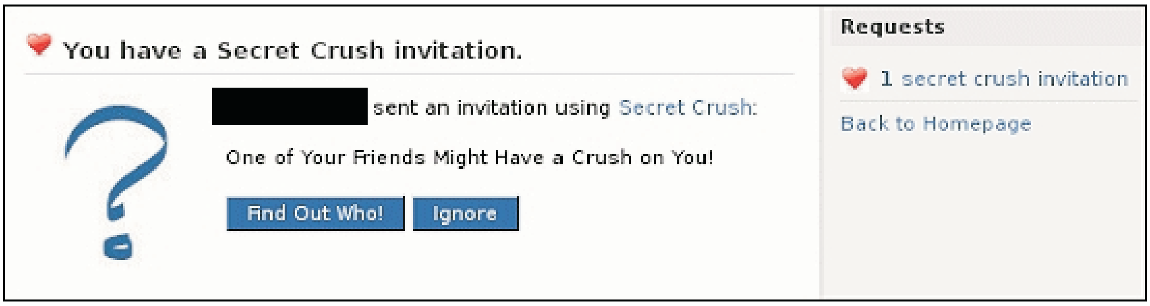
In 2007, an Illinois man posed as an adolescent to befriend young people and exchange photos with them. The man was arrested, and *Facebook* was widely criticized for its failure to protect youngsters.

In July 2007, *Facebook* had yet more security problems. In this case it was a security issue which meant that when a user entered their login details, instead of going to their own account they were taken to the mailbox of another user revealing confidential information of some users.

However the most serious error occurred during December, when *Facebook* claimed that a Canadian pornography company had hacked the accounts of 200,000 users, accessing details such as the username, password and email address.

At the beginning of this year, more than 50,000 *Facebook* were affected by the installation of adware, camouflaged as an additional social networking tool.

Victims received a message claiming to be a "Secret Crush" invitation. However, in order to find out who had sent the message, they were asked to invite another five people to install the application.



You have a Secret Crush invitation.

[redacted] sent an invitation using Secret Crush:

One of Your Friends Might Have a Crush on You!

Figure 15. Image of the "Secret Crush" invitation.

Social networks in the spotlight

Once they had made the five invitations, instead of finding out the identity of their secret admirer, they were told to install another additional application called Crush Calculator, which contained the adware.

In February, a rather unusual case of identity theft in *Facebook* came to light. A 26 year-old IT engineer was sentenced to three years in prison for stealing the identity of Moulay Rachid, younger brother of the King of Morocco.

In March this year, a group of hackers launched an attack against *MySpace* and *Facebook*. This attack took advantage of an exploit in the ActiveX control for posting images on profiles. The vulnerability allowed attackers to overflow the buffer of the control, and include their own commands.

Trojan in *Orku*t

Also in February, a Trojan detected as Orkut.AT used the *Orkut* social network to propagate. The process was as follows:

First, a profile appeared in the targeted user's scrapbook, containing an image from a YouTube video of 'Giselle', a participant in the Brazilian version of Big Brother.

This in itself is a clear indication of how cyber-crooks still find social engineering one of the most useful techniques for spreading malware.

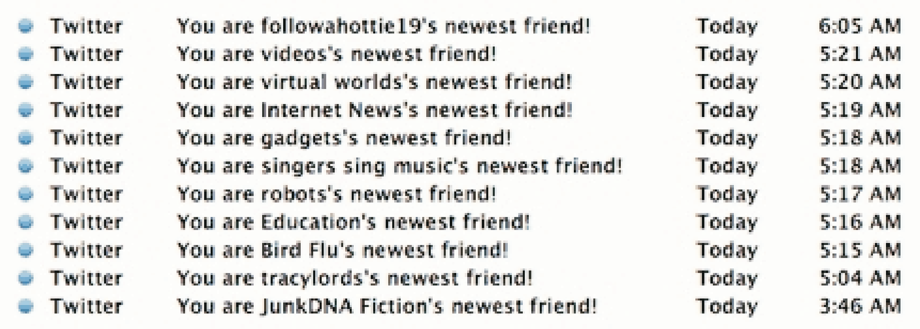
In this case, if the user clicked the link, a message appeared informing them that the video couldn't be played as the corresponding codec was missing. Users were then asked to download it. However, they would really be downloading a copy of the Trojan. To avoid arousing suspicion, while the Trojan was downloading users would then be redirected to the page showing the promised video.

Once in the targeted computer, the Trojan posted a malicious message in the scrapbook of all the victim's *Orkut* contacts.

Social networks in the spotlight

Spam in Twitter

As mentioned previously, spam has also reached social networks and at the end of May, a series of spam messages were detected in *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 16. Spam messages in *Twitter*.

Twitter users received waves of emails through the *Twitter* internal system, advising of the existence of new followers. The problem was that these profiles really contained spam-type adverts. So when a user tried to see who the new follower was, all they saw was spam.

Practical tips for using Social Networking Sites

Nowadays, social networks have become a important target for cyber-crooks. For this reason, users should be alert of possible attacks and follow some instructions in order to use social networking sites in a safe way.

Apart from the basic security measures such as having a security solution installed and keeping up-to-date, there are other measures that can help to prevent these attacks. It is advisable not to share confidential information, such as email addresses, login details,

if you access forums and chats to exchange information, talk, etc. On the other hand, it is also advisable to only provide the information necessary in the profiles. If the site requests private data like an email address, select the option to prevent other users from seeing the information, to ensure no users other than yourself and the administrator can access your data.

Without being aware, users provide many personal data which can make cyber-crooks' work easier in order to carry out fraudulent activities.

Finally, we have considered interesting to add to this report an article we published about the collective intelligence, one of the most important innovations of Panda Security's new 2009 product line.

Collective Intelligence

The main change in Panda Security's 2009 product line with respect to previous versions is "Collective Intelligence". Next, we will explain the reasons for us to embark on this technological evolution.

Current situation

Let's start with the facts. Antivirus programs are subject to the following criticism:

- They are reactive with regard to the appearance of new threats.
- They consume too many resources.

Being reactive is a consequence of the main technology included in all antivirus products: signature-based detection. Basically, this technology consists of incorporating signatures that allow the product to recognize malicious code in files. Even though this is a very old technology, used in the very first antivirus programs, it has been extremely effective. It has however a serious disadvantage: you need to have previous knowledge of the malicious code to be able to add its signature, test it and make it available to users.

With the huge amount of current malware in circulation, there is an issue that all antivirus companies have, but few are willing to admit: if we only protect against the malware that we know, there is a high possibility that our clients are infected by new malware still unknown to us. Add this to the fact that malware has proliferated exponentially over the last few years, and you will be left with an unpleasant scenario. What is worse, all this is mainly based on hypotheses ? even though you can be sure the situation is just as described, you have to prove it scientifically to say it is really a problem to tackle.

This has been a known issue for many years, and, in fact, most anti-malware companies have been developing new technologies to detect the new malicious code that appears without having to depend on signatures. We are talking about old technologies, like heuristic technologies, and more recent ones like behavior analysis.

This takes us to the second criticism above: high resource consumption. Threats evolve over time and antivirus companies must adapt to this. Such is life, however, this might have some disastrous collateral effects. Viruses appeared and so did antivirus programs. All types of threats emerged and antivirus vendors started integrating all kinds of new technologies into their products to combat them: firewall, anti-spam, anti-spyware, heuristics, behavior analysis, content filtering, etc. The appearance of millions of new malware strains has multiplied the size of the signature file that needs to be loaded into the PC memory. Recently, most companies have started to add some new features to products, like backup copying or tune-up options. Even though we do this with the best of intentions, trying to offer users the best protection, we are overloading computers with mammoth tasks.

Collective Intelligence

The birth of Collective Intelligence

Antivirus companies laboratories, besides analyzing new files and creating signatures to detect and disinfect them, develop technologies to detect new malware specimens. At present, PandaLabs has a system that classifies most files we receive: in 2007 we managed to add signatures for 94.4% of all new malware with this system.

The question seems obvious: Why not integrate this into the antivirus programs we sell? Wouldn't we protect users better? Yes, we would, but the process capacity required would be so huge that it would be impossible to integrate it into desktop PCs. Bear in mind that this technology should be added to everything that is already on the computer, saturating it.

With all this in mind we started to sketch out the Collective Intelligence concept. What if we free the local PC from the calculation and decision-making work and leave all that effort in the hands of our servers? The idea was really tempting, and it could greatly increase our detection capacity: currently, when you look at a file in execution you examine it on the PC where it is running. That's the information the antivirus will use to return a verdict on the file's nature. Sometimes there is not enough information and it is not possible to take a final decision on whether a file is good or bad. However, if you have a central repository where you can correlate all evidence about a single file, or similar files, you will have much more information available to return a verdict.

Putting ideas into practice

In theory, all this is fantastic, however, it is when you try to put all this into practice that problems arise: What infrastructure is necessary? What information can be obtained while respecting each country's laws? However, these small problems wouldn't stop us from reaching our goal. The idea was simply too good to dismiss so quickly.

Regarding the information to obtain… Well, this turned out to be very simple. During our internal meetings, someone suggested we would need to upload all files to our servers to analyze them there. Nothing could be further from the truth. To be able to classify a file all you need is an identifier and some information about it. If you analyze a 2 kb file you will need a few bytes of information, and the same applies to 10, 20 or 100 MB files. However, you don't even need to have a part of the file, but a checksum. This way, the information to be sent is reduced to the minimum and we make sure we don't collect any personal data.

Collective Intelligence

First proofs of concept and empirical demonstration of the problem

Last year we released a proof of concept of this technology: a Web-based antivirus that didn't have a signature file and took up less than 400KB. It just performed on-demand scans of files running in memory, and even as such, it was greatly received. After some time, we decided to study the data obtained and check if the capacity of this new concept lived up to our expectations. The data obtained was very good but also very worrying.

On every computer where a scan was performed, a query was made to the Windows Security Center to find out if there was an antivirus installed, if it was active or not, if it was updated, etc. When it came to analyzing the data, we separated the computers that didn't have an installed, activated, up-to-date antivirus. We also started to draw up data by antivirus vendor. What was the result? Clients of ALL antiviruses (Panda included) were infected. We published a white paper with all the data, but here is a summary of the most interesting conclusions:

- Only 37.45% of all PCs had an active, up-to-date antivirus..
- Over 23% of scanned computers with an active, up-to-date antivirus had malware in memory. By malware we refer to all kinds of threats: viruses, Trojans, worms, spyware, etc.
- These are the infection percentages by antivirus company:

CA:	23,32%
McAfee:	24,18%
Panda:	15,54%
Symantec:	22,20%
Trend Micro:	17,08%

The companies appear in alphabetical order as this is not a ranking. The study contained a total of 30 companies, all of them with infection rates between 12-13% to 30% approximately.

Collective Intelligence

Integration of Collective Intelligence in our products

After all this the path to follow was very clear, so we started to apply these technologies to the 2009 product line that we were developing. What is the difference between these products and the previous ones? The most revolutionary change is the integration of Collective Intelligence. What benefits does it offer?

- Optimized signature file (which is loaded into memory to detect known malware).
- Connection to Collective Intelligence when scanning, to maximize malware detection.

The figure below shows the system's basic functioning:

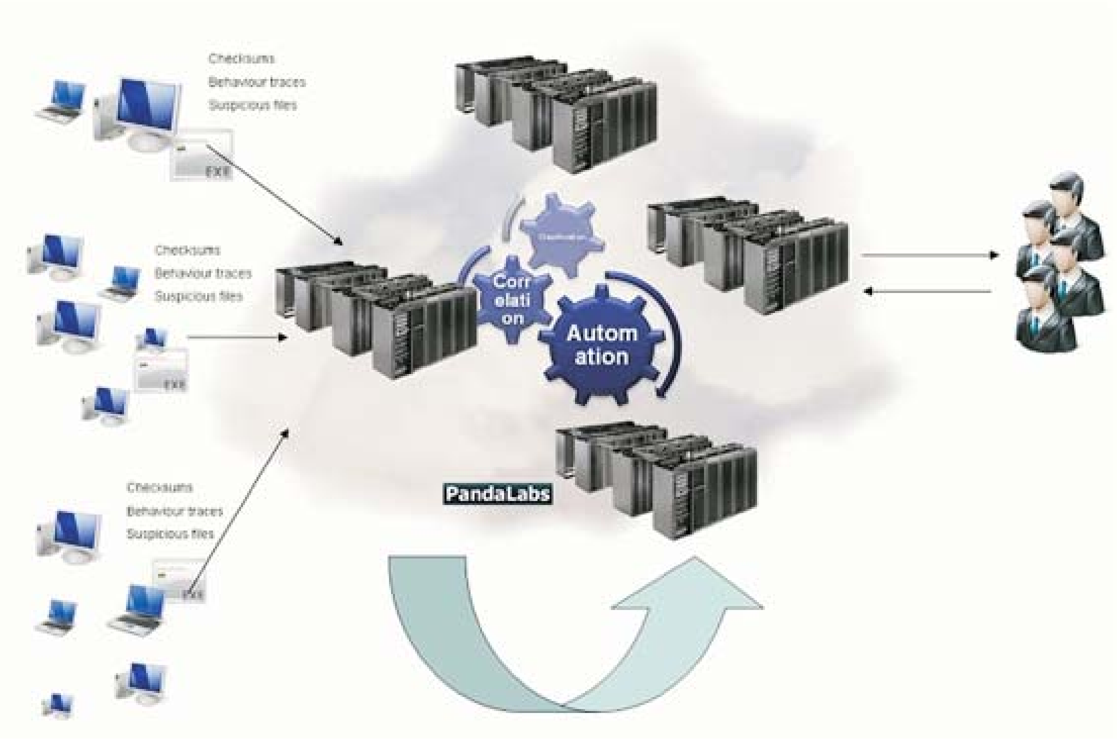


Figure 17. Graph representing the system's basic functioning.

Collective Intelligence

On top of all this, there is TruPrevent 2.0: the fusion of TruPrevent 1.0 with *Collective Intelligence*. The first version of TruPrevent technologies was designed to complement antiviruses, helping them to stop unknown malware. To do this, these technologies analyzed the behavior of all the programs that bypassed the antivirus scan, blocking those that carried out harmful actions and turned out to be unknown viruses.

TruPrevent 1.0 scanned all potential threats using different techniques, carrying out complementary, in-depth analyses at different levels of the infrastructure. Technologically speaking, TruPrevent consists of two main components: behavior-based analysis and blocking.

Panda released this technology in 2004. Since then, four years have gone by of constant innovation and improvement to finally release this new version. This version's engines (heuristic, behavior scanner, etc.) have been adapted to the current malware by using new sensors, etc. Also, every time they detect something they launch a query to the cloud for information about the file. TruPrevent is therefore more effective when it comes to detecting malware, producing almost zero false positives.

To sum up, TruPrevent has been adapted to the current malware situation, characterized by an avalanche of new malicious code every day. This new technology detects and blocks a larger number of strains with less consumption of PC resources. This is due to the fact that most information is hosted on Panda's servers, not on the user's PC.

Questions and answers

When new technologies are introduced on the market, there are always questions that need to be answered. Here is a summary of the most frequently asked questions:

Q: What is an 'optimized signature file'?

A. PandaLabs uses a network of over 4,000,000 sensors to know which malware is currently in circulation and select the necessary signatures to protect PCs against genuinely active malware.

For example, a proof of concept of a malware sample created in 2000 which has never been detected as being active by our sensors will not be included in the signature file. However, a virus that appeared in 1995 but has been active will be included in it.

In any event, Collective Intelligence includes millions of signatures not only of malware, but also of millions of known good files, which provides us with the largest detection capacity

Collective Intelligence

But there is more: TruPrevent proactive technologies, even though they benefit from communicating with *Collective Intelligence*, don't need to be connected to the Internet to detect and stop unknown malware.

Conclusion: Triple protection → Signatures + TruPrevent + *Collective Intelligence*, taking up less resources.

Q: Why is it necessary to keep using the signature file, if *Collective Intelligence* includes all of the signatures?. Couldn't you eliminate it?

A. *Collective Intelligence* requires an open Internet connection. Even though it is true that over 99% of today's infections come from the Internet, there is a small risk window when the Internet connection is not open but you introduce files into the system using a storage device, from a CD to a USB device. That's why we keep using the signature file that contains all active malware, to keep you protected from those attacks.

Q: As my computer needs to keep in touch with *Collective Intelligence*, won't this affect my Internet connection due to the bandwidth required to perform queries?

A. No. As I explained before, only a few bytes are needed for each file. The answer to the query will also take a few bytes as well. Also, this is a smart system which creates a local cache to avoid querying about the same files over and over again.

Q: I understand that thanks to *Collective Intelligence* the product will use fewer resources. However, won't I notice a certain slowdown in my computer due to the communication between my system and *Collective Intelligence* every time a new file arrives?

A. No. The system has been designed to increase detection capacity and reduce resource consumption. The antivirus products that don't use this technology are more resource intensive.

Q: So then, am I completely protected now?

A. No. I don't want to be ambiguous about this. NO. There is no technology today that can give you a complete protection guarantee. Having said that, however, my personal experience tells me that this is the technology that offers the best protection on the market.

Collective Intelligence

Near future

And now what? The truth is that the original idea we had is not totally reflected in the 2009 products, as we are very ambitious. I cannot give you all the details right now, but let's say our idea is something more like Nanoscan: a tiny, extremely light antivirus. We are convinced we are working in the right direction: Trend Micro has recently announced it is going to release products that will connect "to the cloud", and I am sure other competitors will join us over time.

Finally, *Collective Intelligence* has another benefit that I haven't mentioned yet but which many of you will have already guessed: if we create new malware classification and detection systems, we will be able to apply this technology to all our products transparently, as the new technologies will be applied to our *Collective Intelligence* systems instead of to the products installed on our clients' PCs.

About Pandalabs

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

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