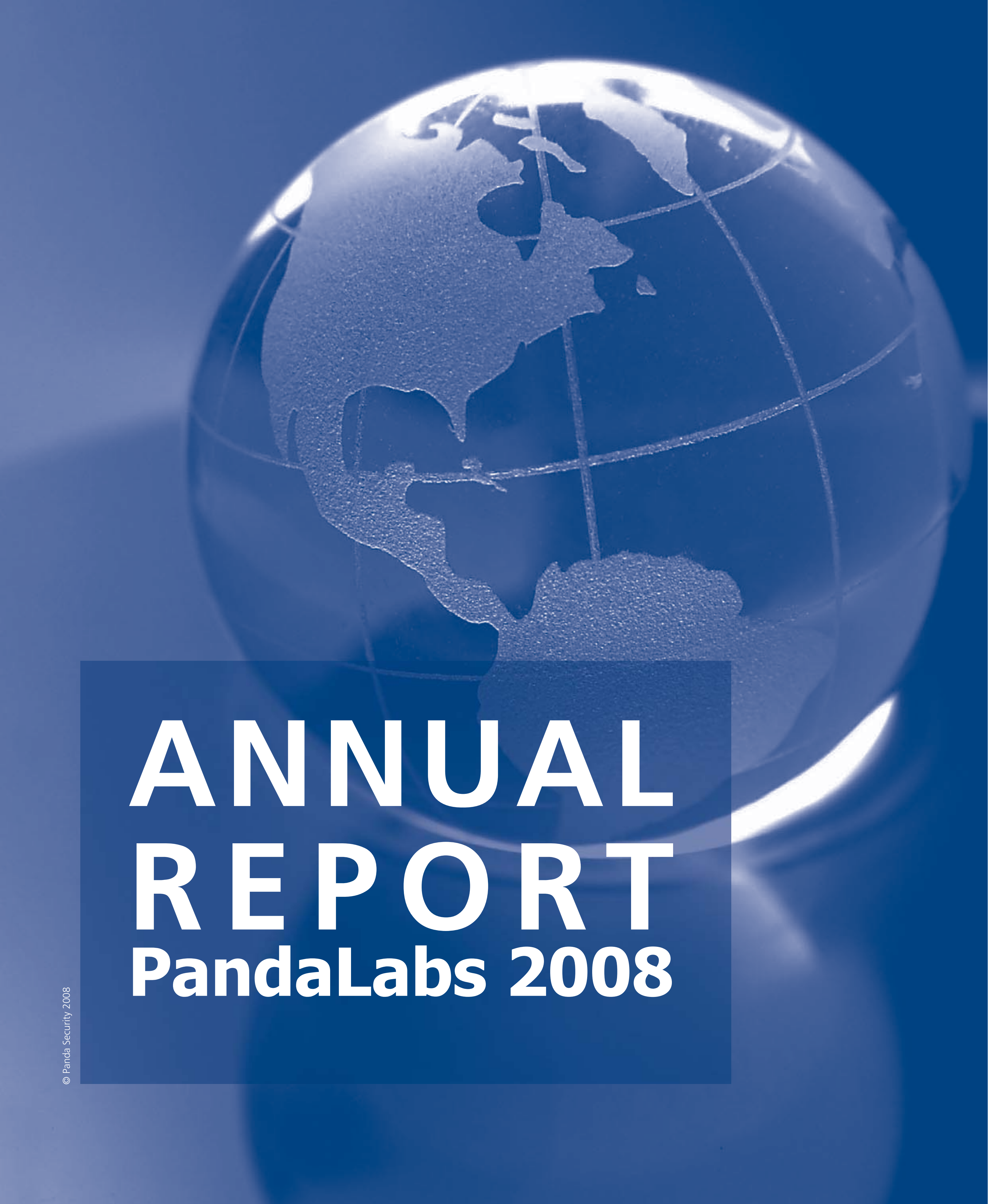


ANNUAL REPORT PandaLabs 2008

PANDA SECURITY | One step ahead.

www.pandasecurity.com

Index

Introduction

As 2008 comes to an end, we present the last quarterly report, giving us the perfect opportunity to summarize the most important events of the year. We will offer the most relevant data in Q4 and analyze the evolution of malware throughout 2008.

In addition to malware, spam has also given us something to talk about this last quarter. Although in this case the news is positive, as with McColo out of action, the volume of spam in circulation reduced considerably. Sadly, however, this would appear to be a temporary blip, as at the time of writing, levels of spam have returned to normal.

A major vulnerability discovered in the RPC service led Microsoft to take the unusual step of issuing a patch outside of its normal monthly cycle to resolve the issue. This vulnerability allowed a network worm to spread in record time. For further information, check out the vulnerabilities section.

Fake anti-malware products have proved to be one of the rising threats of 2008. Along with banker Trojans, they have been among the most profitable resources for cyber-crooks. We have prepared two interesting articles about these lucrative malware families.

Finally, the report includes an article detailing the most notable trends of the year and looking forward to what the New Year might bring.

Similarly, as in previous reports, we outline the evolution of active malware country by country during 2008 as well as the statistics for this last quarter.

We hope you find it interesting.

Executive summary

Trojans were once again the dominant malware category during this quarter accounting for 77.49% of malware detected, up almost 18% with respect to the previous quarter.

With respect to active malware, during the first half of the year, infection rates in Spain and the USA exceeded 40% although the annual averages were 29.17% and 24.36% respectively.

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

With the fall of McColo, levels of spam monitored by Panda Security dropped between 50% and 70%.

In the first eight months of 2008, PandaLabs had already detected more malware than in the entire history of the Panda company, with an average of 22,000 new strains appearing everyday.

Figures for Q4

Distribution of new threats detected

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

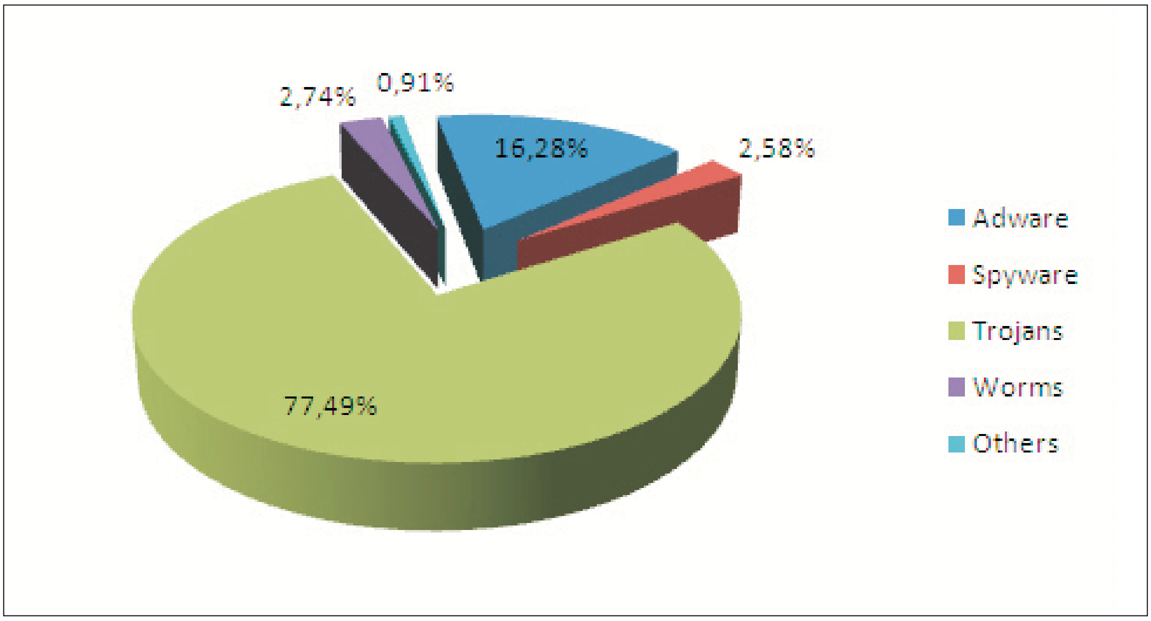


Figure 1. Malware detected in Q4.

As illustrated in the graph, the predominant malware category throughout Q4 has been Trojans, accounting for almost 80 percent of all new variants and up nearly eighteen points on the previous quarter.

Trojans have risen to the fore largely due to the change in motivation of malware creators. Whereas previously they sought notoriety, these malicious programmers are now solely interested in profiting financially from their activity, and to this end Trojans are a very useful tool.

Cyber-crooks distribute thousands of broadly similar variants of a Trojan in order to saturate security companies. However, among this avalanche of malicious code, they will occasionally release a strain of malware that is radically different in the hope that it will go unnoticed and therefore have a longer useful life.

Figures for Q4

Distribution of new threats detected

We have detected several constructor tools this year; Vítrea, YFakeCreator, Wormer, Turkojan… These tools allow cyber-crooks to create new malicious codes practically automatically, without requiring knowledge in programming languages.

With respect to these figures, backdoor Trojans have been included in the Trojans category, and bots have been included in either worms or Trojans, depending on the type.

As for worms, their percentage has decreased by 1.79%, now accounting for just 2.74% of all malware.

Malware creators are still focusing heavily on hybrid worm-Trojans, with the aim of exploiting the characteristics of both these categories to the maximum.

Although adware has declined, there has been a considerable increase in Malware Rogue AV, a subtype of adware, which we will discuss later.

We have grouped categories with low prevalence under the heading 'Other'.

Figures for Q4

Distribution of new threats detected

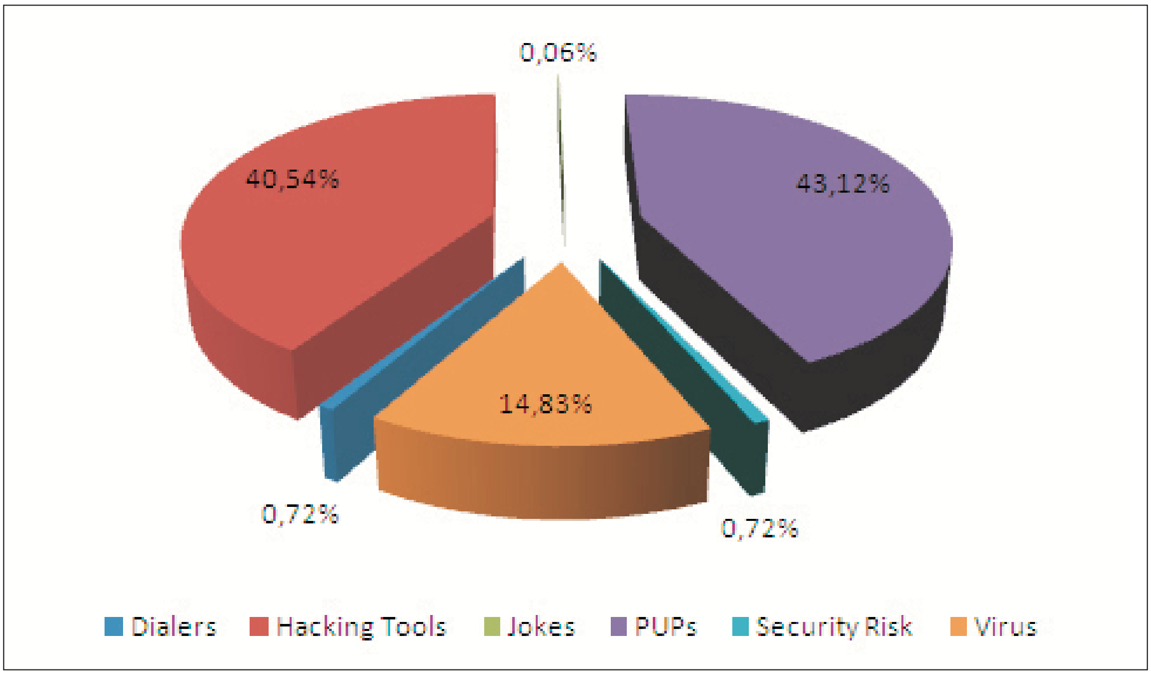


Figure 2. Other malware.

Hacking tools and PUPs (potentially unwanted programs) are the leading malware in this section, at 40.54% and 43.12% respectively. Next come viruses at 14.83% having increased by 3.87% with respect to the previous quarter.

Due to the steady decrease of dial-up Internet connections, the presence of dialers remains negligible.

Figures for Q4

Month by month

Below you can see the appearance of new malware month by month, separated into the most important categories:

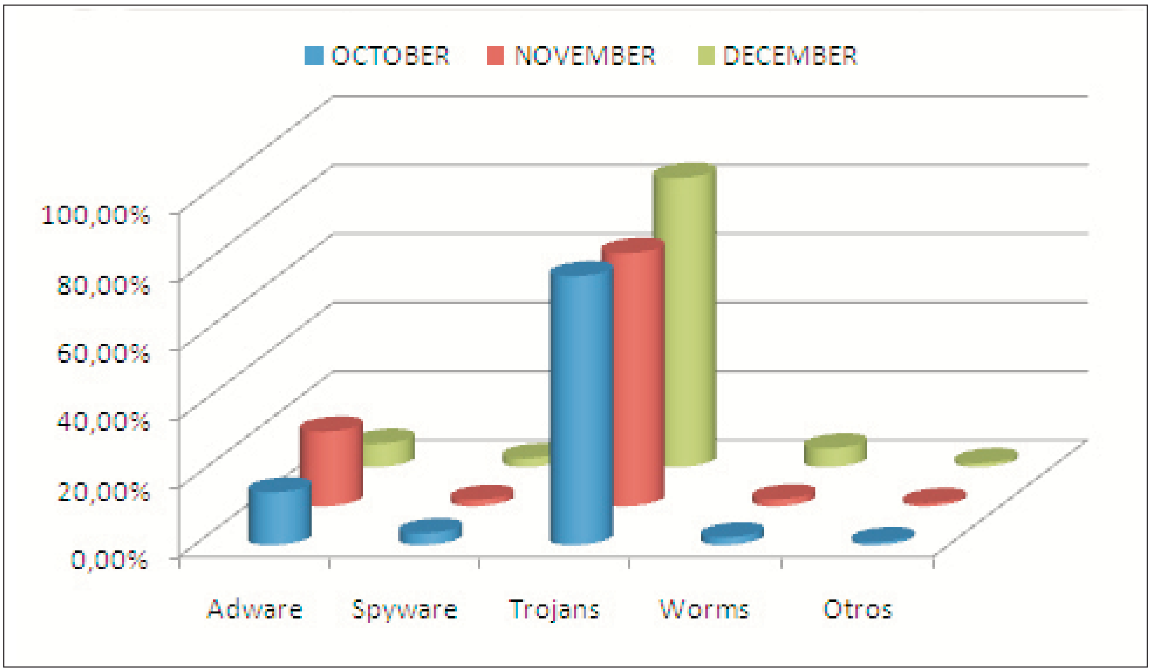


Figure 3. Evolution of the new malware.

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

Figures for Q4

Malware evolution during 2008

Below you can see the appearance of new malware during 2008, separated into the most important categories:

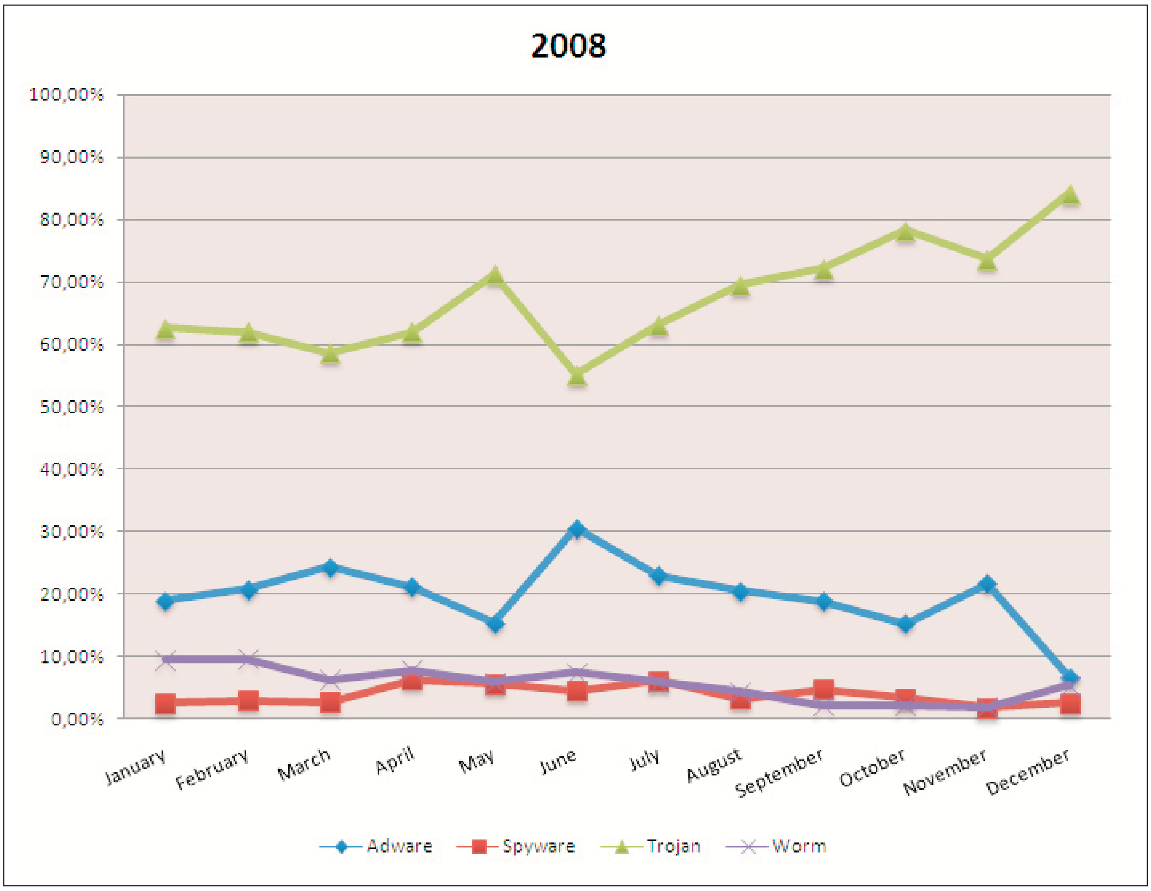


Figure 4. Evolution of malware (annual).

* The December data only includes the data for the first 10 days, therefore the graph does not show each month's real percentage.

This graph further proves that Trojans are the type of malware most widely used by cyber-crooks, as it is the category that provides most financial returns (directly and indirectly).

Figures for Q4

Threats detected by the PandaLabs sensors

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

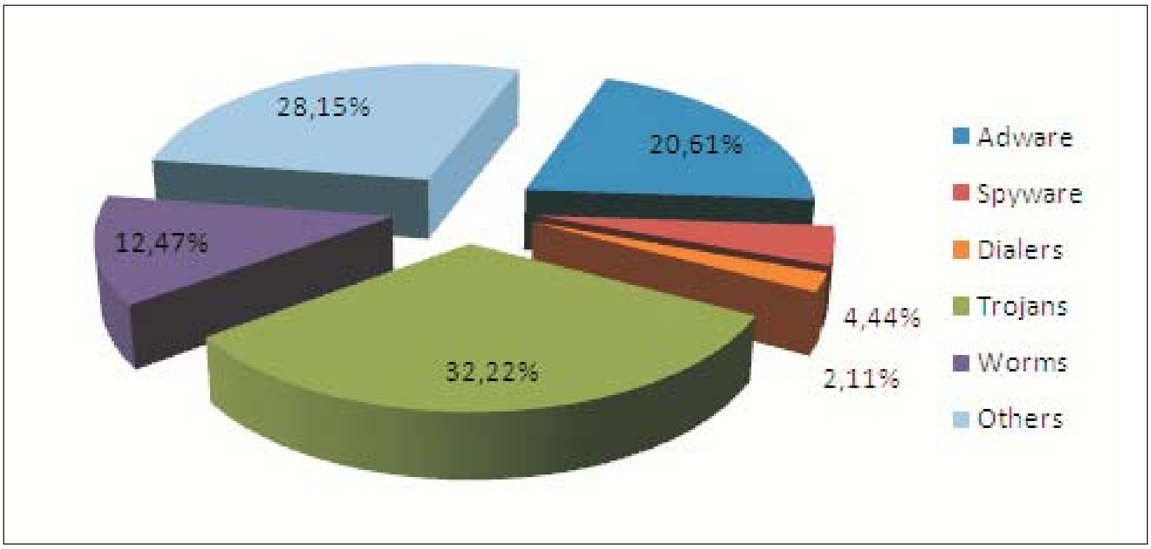


Figure 5. Distribution of detections in Q4.

In this quarter, adware has decreased almost 17% down to 20.61%, with Trojans now in first place at 32.33%. Trojans have increased 3.52% compared to the previous quarter, becoming the most frequently detected type of malware.

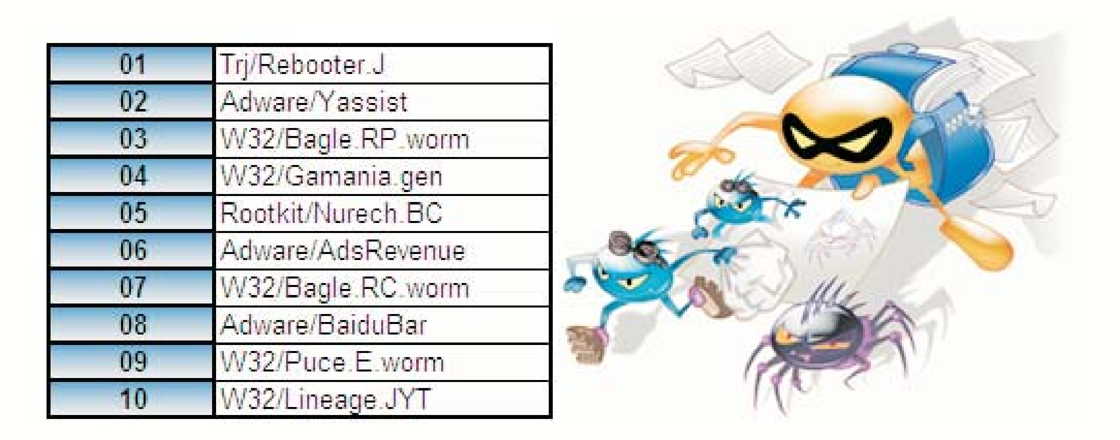
Although worms have increased 0.91%, their infection ratio remains more or less unchanged at 12.47%.

At 4.44%, dialers still refuse to disappear, despite their downward trend since the beginning of last year.

Figures for Q4

Threats detected by the PandaLabs sensors

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



01	Trj/Rebooter.J
02	Adware/Yassist
03	W32/Bagle.RP.worm
04	W32/Gamania.gen
05	Rootkit/Nurech.BC
06	Adware/AdsRevenue
07	W32/Bagle.RC.worm
08	Adware/BaiduBar
09	W32/Puce.E.worm
10	W32/Lineage.JYT

Figure 6. The 10 threats most frequently detected.

Active malware

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

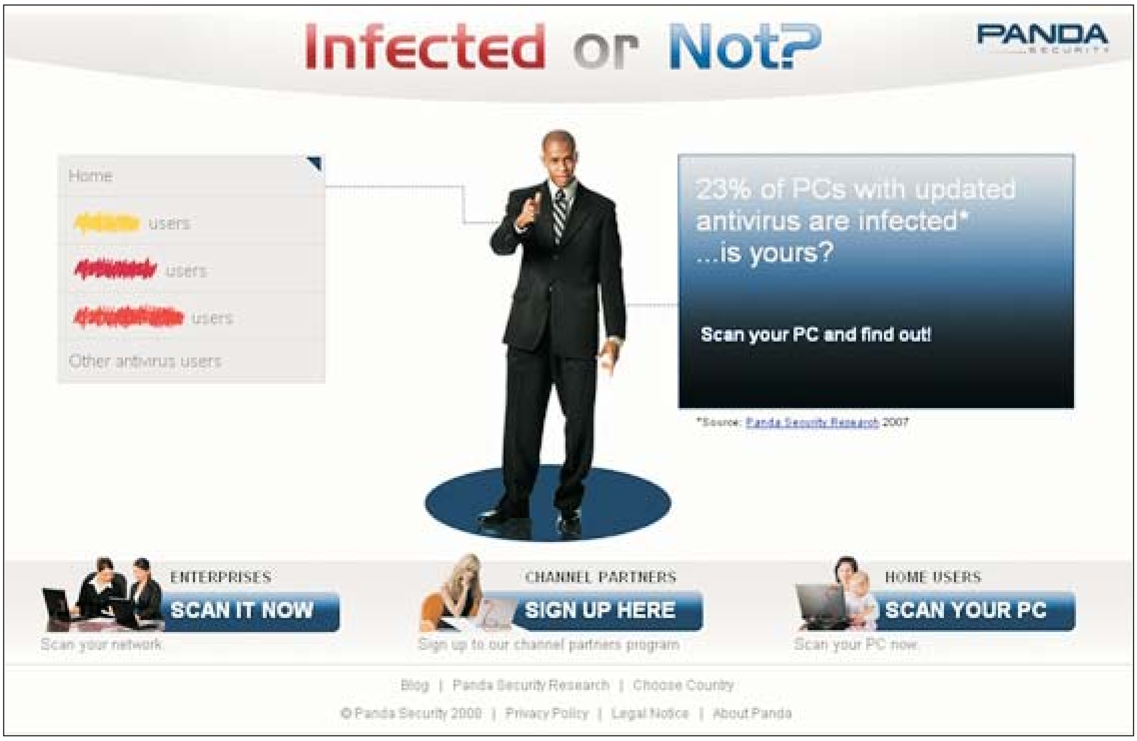
In order to understand what active malware is, we must first define the two possible statuses for malware: active and latent.

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 7. Infected or Not website.

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.

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

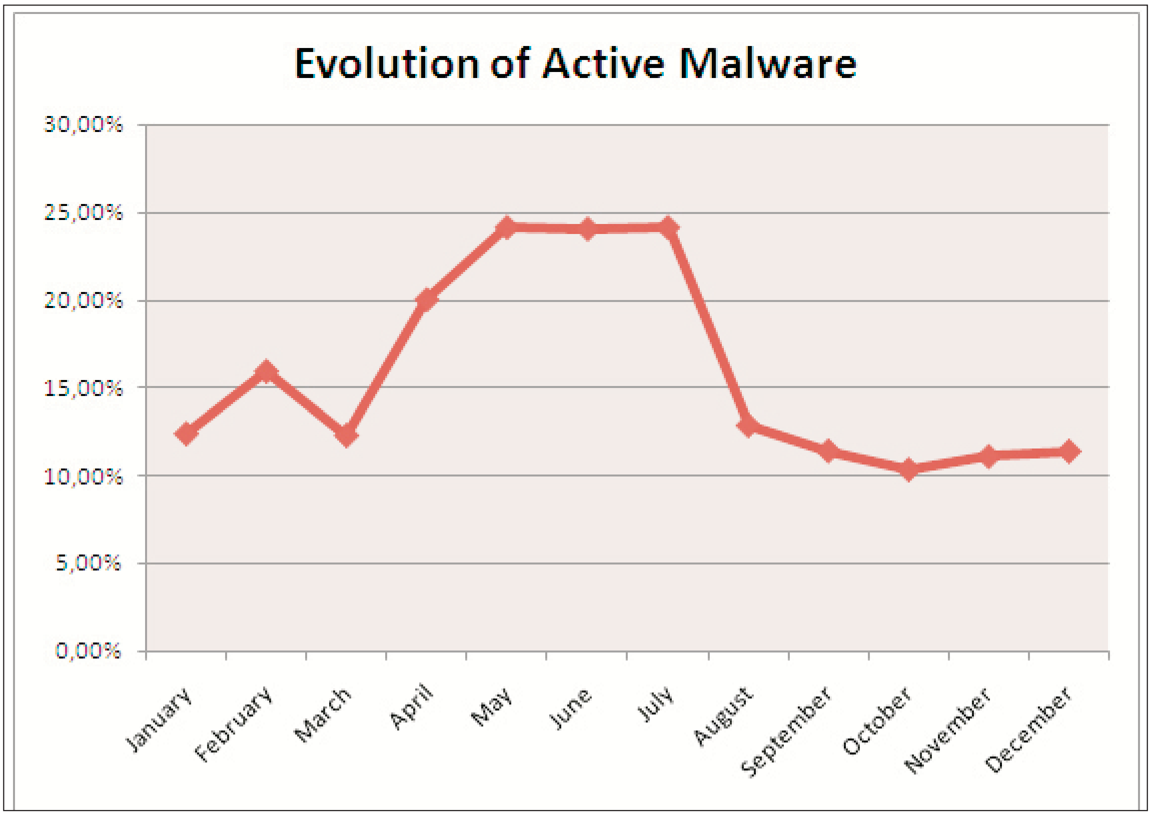


Figure 8. Active malware evolution during 2008.

Q1 was relatively calm regarding active malware, but from then on there was a constant increase. In May, June and July the highest percentages of active malware were reached (around 24%). After that there has been a progressive decrease, reaching the lowest percentage in October (10.31%) and ending the year at around 12%[1] (in December).

[1] Data gathered up to 10/12/2008.

Active malware

At present the average active malware is at 15.48%, almost 2% less than in the first semester (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:

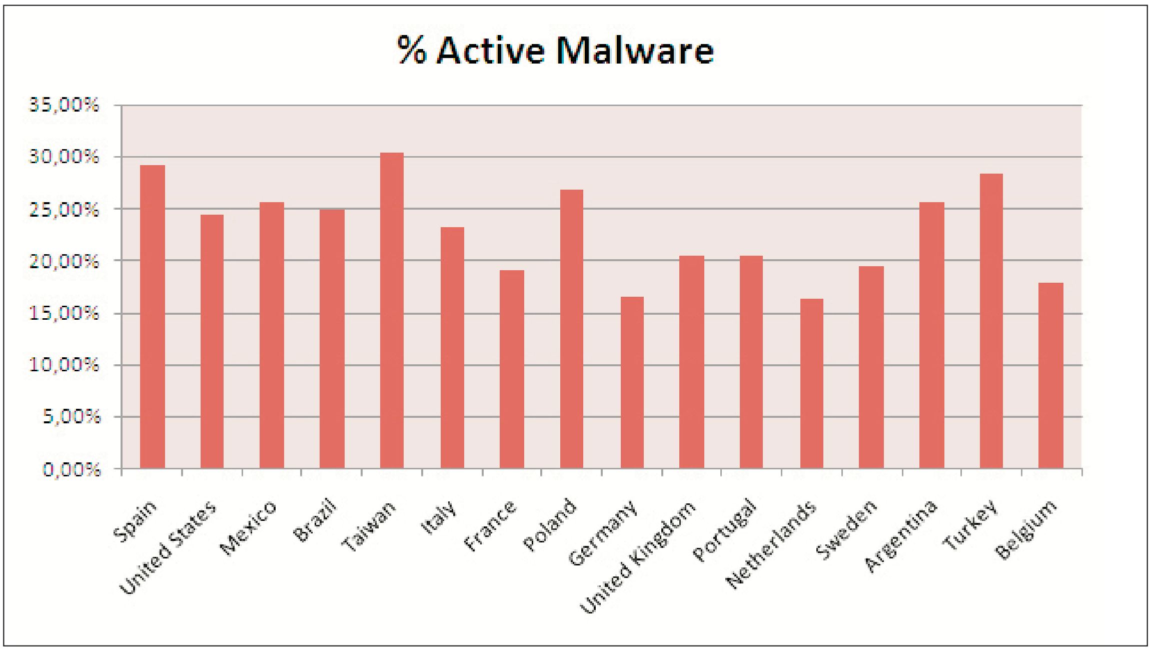


Figure 9. Countries with highest malware percentage (January-December).

In the first semester all countries exceeded 30% infection rates, and some were over 40% as was the case of Russia, Spain and Mexico. In Q3 the situation improved, Spain and United States being the countries with most active malware, but with much lower infection ratios (around 30%).

On the whole, infection percentages in the countries have decreased in 2008, especially in **Spain** and **United States** who were above 40% in the first semester and finally ended up with a yearly average of 29.17% and 24.36% respectively.

Although the infection ratios in Spain have considerably decreased, it is still together with Taiwan and Turkey one of the countries with the highest active malware percentage.

This data is positive, as it shows an improvement in active malware after the alarming ratios of the first semester. At present, only Taiwan is above 30%. Overall, this year's evaluation is satisfactory.

Current spam status report

At Panda Security we are aware of the importance spam-filtering systems have for our clients. Consequently, our groundbreaking research departments, such as PandaLabs, are making incredible efforts to ensure our anti-spam solutions meet our clients' needs and are ahead of other anti-spam solutions in the market.

In this final report of the year we would like to draw your attention to an important fact regarding spam; the crash of several systems belonging to the McColo ISP and its consequences. We would also like to stress the effort Panda Security is making to combat new threats such as illegitimate NDRs (also known as backscatters).

The end of McColo

As mentioned in the Q2 report, in the first few months of 2008, spam accounted for 60-94% of emails sent through the Internet. We also mentioned botnets were the most common method for distributing spam.

The situation has drastically changed in the last quarter. On November 11, North American authorities shut the McColo Internet Service Provider down, as it was used by a large number of cyber-crooks, and its domains were used to control botnets to distribute malware and send spam (directly or indirectly).

From that day on, the amount of spam circulating the Net decreased considerably; spam levels monitored by Panda Security dropped 50-70%.

Apart from lower spam figures, there were also changes in the nature of spam. Up until November 11, the spam distribution in our monitoring systems was as follows: 50% only text (plain and HTML) and 50% emails with attachments (some of which were malware).

From November 11, the spam profile has changed towards the dominance of exclusively text content. From this it can be deduced that McColo was not only an important source of spam, but also of malware distribution, as from that week on, the distribution of certain fake anti-malware families also subsided.

Current spam status report

At PandaLabs, we did not doubt the decrease would be temporary and that alternative ISPs would be used to perpetuate malicious activity. Since then, we have seen spam levels return to normal.

As Christmas approaches, spam levels are expected to reach the figures previous to McColo's shutdown. The nature of spam however, is not expected to change, but to continue consisting mostly of text.

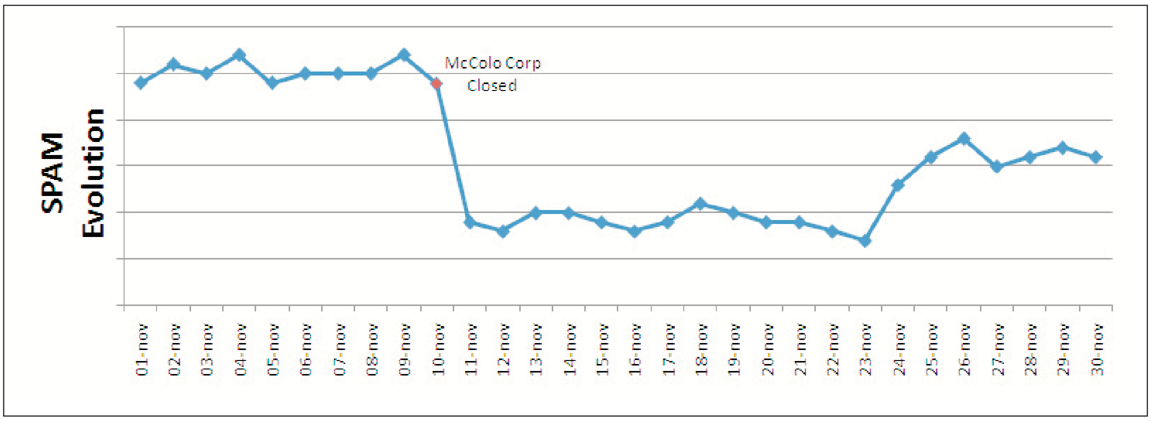


Figure 10. Spam levels during November.

New threats: NDRs

This year we have mainly focused on improving our junk mail (spam and backscatter) detection systems. Our spam detection ratios are still optimum and we also continue to investigate and improve our solutions to detect more, and for our detection systems to be more stable on specific occasions or when facing waves of spam.

This year we have also talked about NDRs (Non Delivery Reports) and have explained their origin and functionality. Illegitimate NDRs are unwanted emails that cannot be considered as spam, since they consist of emails generated by legitimate mail systems, as mentioned in the previous quarterly report.

To this end, we continue to work and try different technologies to implement systems that can differentiate between legitimate NDRs (generated from an email sent by the user) and illegitimate NDRs (generated from an email sent by a spammer).

Next year these improvements will slowly see the light, allowing our clients to benefit from an even better service.

Main vulnerabilities in 2008

This section summarizes the most important vulnerabilities in 2008. We also explain the most popular methods of malware distribution used to exploit these vulnerabilities during the year.

Overview

This year has seen the appearance of several vulnerabilities that affected Microsoft Office; some of them were discovered "in-the-wild", that is, before the vulnerability was made public. This type of vulnerability appears year after year, together with vulnerabilities affecting web browsers such as Internet Explorer, Firefox, Safari and Opera.

The latest addition to this set of vulnerable applications was Google's beta browser: Chrome. However, the fact that numerous security flaws were reported just a few days after the application release cast many doubts on the security of Google's application. Let's see what happens when they launch the final version.

Vista has also been affected this year with various vulnerabilities exploited remotely. Back in February, two flaws were reported that affected Internet Information Server (IIS) and allowed privilege escalation and remote execution of code.

Nevertheless, Microsoft is not the only company to have been severely hit by vulnerabilities. Adobe has also been affected by multiple security flaws in its products, some of them as critical as to allow code to be run on targeted systems simply by visiting a malicious web page with a flash animation that exploited the vulnerability.

The latest reported vulnerability affects products such as Adobe Acrobat and Adobe Reader. This security hole allows code to be run on affected systems due to incorrect parsing of the javascript util.printf() function used to generate PDF files.

Main vulnerabilities in 2008

Top vulnerabilities

Here are the top 3 vulnerabilities in 2008:

DNS vulnerability

Everyone in the security industry agrees that the vulnerability discovered in the DNS service is one of the most serious discovered this year. This flaw allows malicious users to redirect web pages or domains to a system controlled by the attacker.

After several months of research, Dan Kaminsky discovered a vulnerability that exploited two different issues with the DNS protocol: prediction of source port and transaction ID, and additional resource records. This vulnerability allows attackers to control all traffic sent to a domain.

81 vendors were warned in CERT's advisory. This is said to have been the most important synchronized security update in Internet's history. This was the first time that many of the top companies (Cisco, Microsoft, etc.) worked together to guarantee users' security as soon as possible.

For more information about this vulnerability, read the PandaLabs Q3 report.

ClickJacking, a new threat

This vulnerability was discovered by Jeremiah Grossman and Robert Hansen, two of today's top security researchers. Their presentation at the OWASP APPSEC USA'08 in New York had to be postponed at the request of web browser vendors and Adobe, due to the consequences it could have.

This vulnerability is caused by known design errors in web browsers. The exploit uses targeted users' clicks for actions they were not intended for.

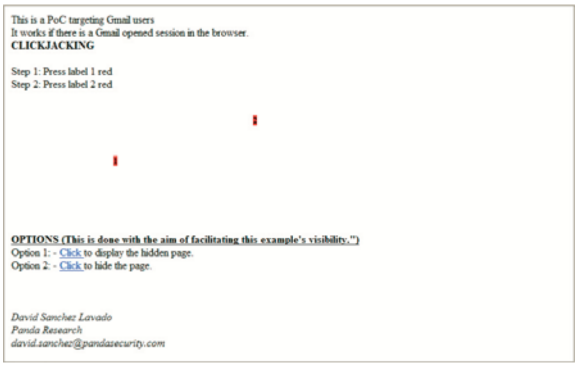
Main vulnerabilities in 2008

Top vulnerabilities

One of these attacks consists of creating an invisible iframe that hides malicious coding beneath apparently legitimate buttons or other clickable content on pages visited by the user: email sites, photo storage sites, etc. A malicious user could create a web page with a set of dummy buttons, then load another page over it in a transparent layer. The user thinks he is clicking the visible buttons, while actually performing actions on the hidden page loaded from the iframe. This could result, for example, in users making their myspace profile public, showing their flickr private pictures or deleting their firewall rules unknowingly.

One of the actions that worried Adobe the most was the fact that, by using this technique, an attacker could activate the victim's camera and microphone and record video and audio without the targeted user knowing.

We reproduced this technique at PandaLabs and saw just how simple it is. We prepared an 'online game' in which users were required to click on certain areas of a web page. However, whenever they clicked the buttons they were performing actions like deleting messages from their mail accounts without realizing.

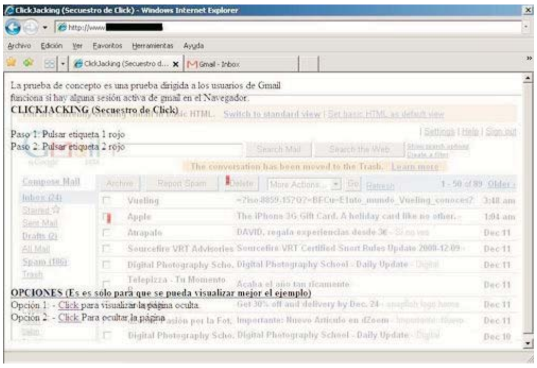


This is a PoC targeting Gmail users
It works if there is a Gmail opened session in the browser.
CLICKJACKING

Step 1: Press label 1 red
Step 2: Press label 2 red

OPTIONS (This is done with the aim of facilitating this example's visibility.")
Option 1: - Click to display the hidden page.
Option 2: - Click to hide the page.

David Sanchez Lavado
Panda Research
david.sanchez@pandasecurity.com



ClickJacking (Secuestro de Click) - Windows Internet Explorer
http://www[redacted]
Archivo Edición Ver Favoritos Herramientas Ayuda
ClickJacking (Secuestro d...
Gmail - Inbox
Switch to standard view | Set basic HTML as default view
Settings | Help | Sign out
Search Mail
Search the Web
The conversation has been moved to the Trash. Learn more
Compose Mail
Archive
Report Spam
Delete
More Actions...
Go
Refresh
1 - 50 of 89 Older ›
Inbox (24)
Starred
Sent Mail
Drafts (2)
All Mail
Spam (186)
Trash

La prueba de concepto es una prueba dirigida a los usuarios de Gmail
funciona si hay alguna sesión activa de gmail en el Navegador.
CLICKJACKING (Secuestro de Click)

Paso 1: Pulsar etiqueta 1 rojo
Paso 2: Pulsar etiqueta 2 rojo

OPCIONES (Es es sólo para que se pueda visualizar mejor el ejemplo)
Opción 1: - Click para visualizar la página oculta
Opción 2: - Click Para ocultar la página

Figures 11 and 12. Clickjacking technique.

Main vulnerabilities in 2008

Top vulnerabilities

Microsoft MS08-067 and the Conficker worm

This vulnerability, together with the DNS flaw, were the most important to appear in 2008. In order to fix this vulnerability as soon as possible, Microsoft had to bypass the company's regular patch release cycle (the second Tuesday of each month).

The vulnerability stems from incorrect handling of maliciously crafted RPC requests. An attacker that exploited this vulnerability could take full control of the affected system.

This flaw affects all Microsoft operating systems, Vista and 2008 Server included, causing a denial of service in both cases. However, the vulnerability is most critical in Windows 2000, Windows XP and Windows 2003 as it grants access to the targeted system through shared resources without any need for authentication. This allows code to be remotely executed. The discovery of this security hole resulted in the creation of the Conficker.A worm, which spreads by exploiting this new, dangerous vulnerability on computers that haven't been patched.

Microsoft states on its website that if the user follows the recommended procedures for using the firewall and the predefined security settings, they will be protected against these attacks. Microsoft also recommends that computers connected to the Internet have as few ports as possible exposed.

Nevertheless, it is strongly recommended to apply the patch published by Microsoft regarding vulnerability MS08-067.

Main vulnerabilities in 2008

Means of infection

This section deals with the various infection methods seen this year. Even though these methods are not new, they are still very efficient for infecting systems.

Method A: Social engineering techniques

Social engineering techniques are usually exploited in emails sent massively, but also in forums and blogs. Vulnerabilities exploited through these techniques are generally due to uncontrolled errors in applications when parsing files, usually office files.

This means of infection requires intervention from the targeted user; for example, by opening a file. Attackers use social engineering techniques that exploit the user's curiosity to trick and infect them. Hundreds of thousands of computers are infected every time a malicious document that refers to some important news circulates the Internet. In this context, it is not difficult to understand why so much current malware uses subjects related to the historic victory of the new US president, Barack Obama.

All of us are exposed to these attacks every day, and, if we are not aware of the consequences of opening an attachment of unknown origin, we will end up infected by some malicious code sooner or later. The biggest danger lies in opening Microsoft Office files, Adobe PDF files and multimedia files.

The TruPrevent technology available in our Antivirus 2009 line is specially designed to prevent these types of unknown attacks.

Here are some of the vulnerabilities used this year to infect users through social engineering techniques:

- Microsoft Word Smart Tag Invalid Length Processing Vulnerability (CVE-2008-2244)
- Microsoft Access Snapshot Viewer ActiveX Control Vulnerability (CVE-2008-2463)
- Microsoft code executión Vulnerability (CVE-2008-1091, CVE-2008-1434)
- Microsoft Word File Information Block Memory Corruption (CVE-2008-0109)
- Microsoft Excel Multiple Vulnerabilities (CVE-2008-3471, CVE-2008-3477, CVE-2008-4019, CVE-2008-3003, CVE-2008-3004, CVE-2008-3005, CVE-2008-3006)
- Microsoft Excel Multiple code Excution Vulnerability (CVE-2008-0081, CVE-2008-0111, CVE-2008-0112, CVE-2008-0114, CVE-2008-0115, CVE-2008-0116, CVE-2008-0117)
- Adobe Reader/Acrobat Javascript Method Handling Vulnerability (CVE-2008-2641)
- Adobe Acrobat/Reader Multiple Vulnerabilities (CVE-2008-2549, CVE-2008-2992, CVE-2008-4812 a CVE-2008-4817).

Main vulnerabilities in 2008

Means of infection

Method B: Infection through legitimate Internet pages

It is often thought that users who do not visit sensitive or dubious web pages cannot be infected. However, the second quarter of the year brought a change to this conception as millions of 'secure' pages were infected with malicious code and infected, in turn, thousands of computers.
At the beginning it was assumed that those incidents were caused by a "zero-day" vulnerability that affected Microsoft Internet Information Servers and Microsoft SQL Servers. This was denied by Microsoft. web applications of infected servers were vulnerable to *SQL Injection attacks*[2] even though the server was completely patched.
These attacks were performed with specially crafted tools that modified the content of the web pages of the application under attack, by inserting an iframe pointing to a server that contained a number of exploits: MS06-014, MS07-004, MS07-018, MS07-033 and MS07-55.

This attack (normally automated) starts by searching for web applications that can be vulnerable to SQL Injection attacks with Google's search engine[3] . Once one or several vulnerable servers are found, the tool launches attacks to identify the design of the database behind the web application. Once it has been identified, a final attack is launched, consisting of modifying the content of the text fields in the tables in the attacked server's databases.

As a result, the web application will contain legitimate information but also malicious code that will run whenever the application's HTML pages are loaded. This code will install malware on the system without the user noticing. As we have already explained, these infections exploit vulnerabilities that affect web browsers or their components.

This method of infection is very efficient and cost-effective for cyber-criminals, who don't have to contract spam distribution services. It is the target user herself that goes to the 'secure' page, which further hides the means and origin of the infection. Moreover, in the case of highly popular pages, cyber-crooks ensure a minimum number of infections.

[2] A technique that consists of injecting SQL sentences into the real SQL query to be run on the database server.
[3] This technique is known as Google Hacking.

Main vulnerabilities in 2008

Means of infection

At the beginning of 2007 hundreds of thousands of users were infected on visiting the SuperBowl website[4]. In 2008, TrendMicro's website was compromised[5], and thousands of users and visitors to the antivirus vendor's website became infected by a Trojan.

These and other examples show that secure pages can also be a source of infection, and this is even more serious in the case of attacks aimed at online banking or shopping sites.

Method C: Network worms

Out of all infection methods, network worms have been undoubtedly the most dangerous over the last few years. Even though the year 2008 looked like a quiet year regarding this type of infection, in October Microsoft published the MS08-067 security bulletin, which referred to a "zero-day" vulnerability that affected all versions of the company's operating systems.

Even though Windows Vista has improved its security features and is the most secure Windows operating system so far, it has also been affected by this serious vulnerability. The flaw causes a denial of service in Windows Vista and 2008 Server and allows for remote execution of code in Windows XP and 2000, which has caused the appearance of new network worms like W32/Conficker.A.worm. Network worms do not require user interaction. Once a system has been infected, the computer takes advantage of other vulnerable computers and spreads across the network automatically.

Finally, this type of infection is not completely transparent, as it is quite usual to detect worm infections on noticing anomalous network traffic, operating system failures due to excessive memory or CPU usage and errors caused in Windows services such as svchost.

[4] http://www.infoworld.com/article/07/02/02/HNdolphinssiteshacked_1.html
[5] http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9068478

Main vulnerabilities in 2008

Means of infection

Summary

Regardless of the malware distribution method, computer attacks are an important source of financial benefits for attackers, as shown by the fact that the distributed malware is mainly designed for stealing bank details.

Malware creators wait until the second Wednesday of each month to exploit "zero-day" Microsoft vulnerabilities and get the biggest impact and duration for their creations.

This way, they have a one-month window until the next Microsoft security update. Nevertheless, on several occasions Microsoft has been forced to skip its update routine and publish an urgent patch to fix a security flaw due to the impact and seriousness of the vulnerability, as it happened with MS08-067.

Panda Security advises users to keep their antivirus solution permanently up-to-date and have a firewall enabled. They are also recommended to apply the latest updates of the operating system, web browsers and all installed applications to increase the system security. Windows XP users are also advised to install Service Pack 3 published by Microsoft and the update that fixes vulnerability MS08-067, as it was released after Service Pack 3.

Report on Banker Trojans

Banker Trojans continue to represent a serious threat to users. Even though many banks have increased security measures on their websites, these malicious codes have become more sophisticated and include new functions.

One of the greatest concerns to users regarding Internet security is the theft of confidential information, such as passwords, particularly those for bank accounts. That's why banker Trojans are considered one of the most dangerous types of malware for Internet users, as they are designed precisely to steal this type of information.

Banker Trojans, along with fake antivirus programs which we also discuss in this report, would appear to have become the most profitable categories of malware for cyber-criminals.

Social engineering continues to be among the most popular means for distributing this type of malware on users' computers. However, user interaction is not always required, as malware can also be distributed through infected web pages.

Once installed on a computer, the main aim of all these Trojans is to steal bank details from victims. The Trojans normally go memory-resident, and only activate when users visit the web pages of certain banks. To this end, the Trojans include a list of banks which they can target.

These programs are readily available to cyber-criminals, as there is an extensive black market in a la carte Trojans and banking malware kits, allowing users not only to create Trojans with multiple functionalities but also to control them and even send them new instructions.

This article examines the main banker Trojan families, explaining how these codes normally enter computers, and analyzing the complex structure that is behind this lucrative criminal business. We also offer a series of recommendations on how users can protect themselves from these threats.

Report on Banker Trojans

Main families

There are many different families of banker Trojans although, broadly speaking, the most active families fall within three categories:

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.

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 the differences between variants created with these tools are minimal, as the kits have not been updated over the last few years.

One consequence of this is that the variants of 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, some of these are the most active families, and as they are continually changing and being updated with the capacity to steal credentials from different banks, they are also the most dangerous. This makes it difficult for antivirus solutions to detect them generically.

All of them have one common function: The list of target banks and organizations is obtained from a configuration file, which can either be included with the Trojan or in a server controlled by the cyber-criminal, 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.

Report on Banker Trojans

Infection channels

Social engineering continues to be among the most popular means for spreading this type of malware on users' computers, and it is often distributed in one of two types of spam messages:

1) Spam with an attachment. These are normally compressed files, with a .zip extension, containing an executable file. However, to trick users into thinking the files are inoffensive, the following techniques are used:

- **Inoffensive icon:** The icon of the file coincides with the type of file that the attachment claims to be. So in the case of an image, for example, the icon would be as follows:

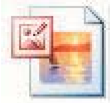


Figure 13. Image icon.

- **Double extension:** Often, the executable file has a double extension. The first extension is that of the type of file that the attachment claims to be, so in the case of an image it could be .jpg, and the second extension would be .exe. There is normally a gap between the two extensions to prevent users from discovering that the real extension is .exe.
  However it is not always necessary to add an inoffensive extension. If the attachment has an icon that is apparently harmless, users may not pay much attention to the extension itself.

Very often, the file executed by the user is a Downloader-style Trojan. These are small files designed simply to connect to a web page to download the real banker Trojan.

2) Spam with links to a web page. These messages often carry links supposedly pointing to a video on the web. When users click to see the video, they are often prompted to install something such as a codec or flash update, etc.

Once the download is made, to allay any suspicions, users may even be taken to a web page where they can see a video, although this is not always the case.

However, early this year we began to see the popularization of a more sinister technique: the infection of legitimate websites. Code is inserted into the web pages which calls and supplies information to a malicious server about the user's operating system, browser and patches installed in order to exploit vulnerabilities and insert malware including banker Trojans.

Report on Banker Trojans

The sophistication of banker Trojans

Banks have responded to the threat of banker Trojans, improving security and client authentication procedures. In consequence, the techniques used by this type of malware to steal information have in turn become more sophisticated.

The use of virtual keyboards for user verification was an important step forward for these secure web pages, as it prevented keyloggers from capturing the data entered by users.

However, it was not long before malware creators developed new functions for banker Trojans, enabling them to trace the movements of the mouse or even make video captures of the screen, as in the case of Trj/Banbra. DCY.

Some strains of malware, such as those of the BankoLimb family, have a file with a list of URLs of target banks. When users infected with BankoLimb access a web page in the list, the Trojan is activated and injects HTML code in the bank’s page.

The result is that users are prompted to provide more information than they normally do when registering. The user is actually on the legitimate web page but it has been slightly modified. For this reason users should be alert to anything out of the ordinary on their bank's web page, because as in this case, any additional information provided will be captured.

In other cases, Trojans can superimpose a fake page over the original or simply redirect users to a spoof website. Once the information has been captured, victims may see an error message or are sometimes even taken to the genuine website of the bank.

Some variants of the Sinowal family are highly sophisticated, and are capable of modifying data ‘on-the-fly’. For example, if the user is carrying out a transfer from his bank's web page, these variants can alter the data of the intended recipient of the transfer once a petition has been made. The result of the operation returned to the user includes the original data, thus avoiding any suspicion.

Other variants consult a server to check whether they should take any action depending on the web pages that the user is visiting. This means malicious code does not depend on a configuration file and cyber-crooks can extend the list of websites from which they steal information or inject code, etc.

Once information has been stolen, it is often transmitted via email or posted to an FTP server.

Report on Banker Trojans

Organized crime

The creators of banker Trojans that steal confidential information are rarely the same individuals that actually steal money. The criminal business model that has evolved around this type of malware is highly complex.

The following diagram illustrates the complexity of the typical structure behind this kind of activity:

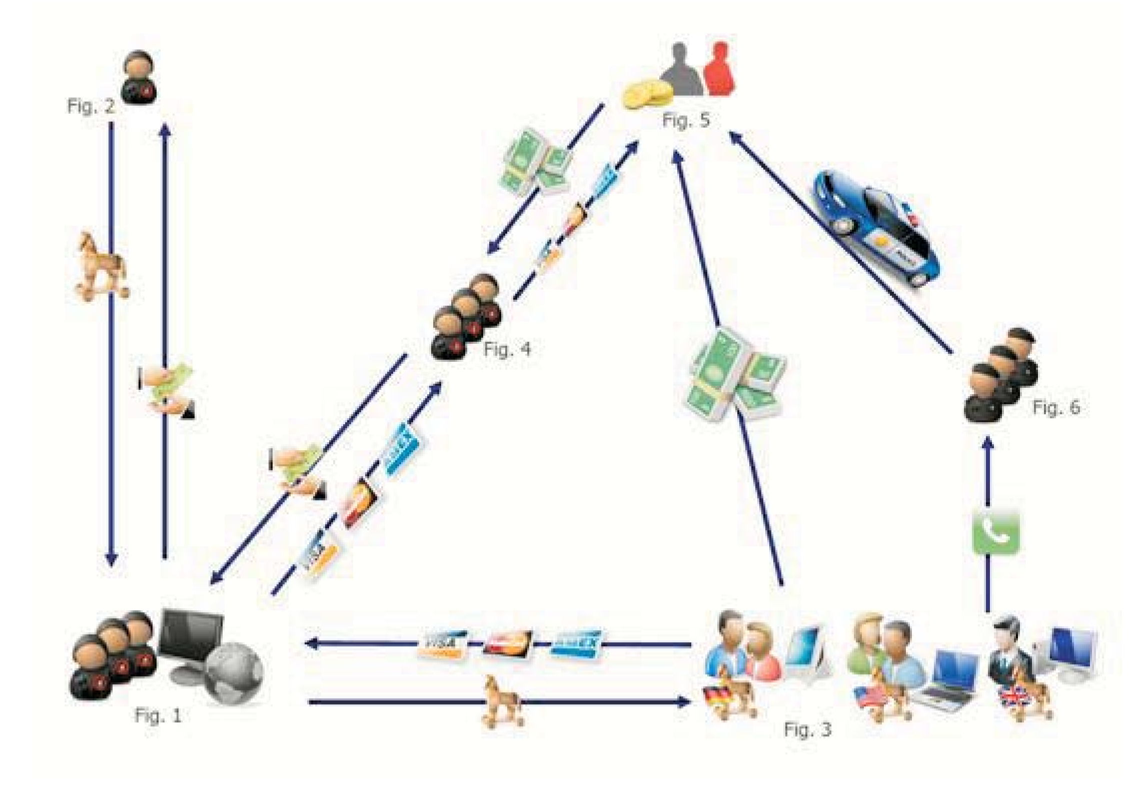


Figure 14. Organized cyber-crime.

Report on Banker Trojans

Organized crime

Below we explain how this structure operates.

Firstly, groups of cyber-criminals (fig. 1) commission a purpose-built Trojan with specific characteristics from specialized forums or the malware black market (fig. 2). They may even rent the entire infrastructure needed to distribute the Trojan, either via spam or malware servers using drive-by-download techniques. Through this technique, files can be automatically downloaded to computers by exploiting system flaws without users' knowledge.

Once they have the Trojan, it is distributed to users to steal their bank details (fig. 3). To this end, the most common distribution methods are spam or infected web pages.

The technique for infecting legitimate web pages involves modifying the source code, by adding an iframe-type reference to a malicious server.

These criminals do not steal money directly from users, they steal their bank details which are sold on to others (fig. 4). This makes it even more difficult for law enforcement agencies to follow the trail.

All of the data stolen is sold on the malware market. However, neither do those who buy the stolen bank details actually steal the money. To cover their tracks yet further, they contract other people who act as intermediaries -money mules (fig.5)-, contracted under the pretext of working from home.

The money stolen is transferred to the accounts of the money mules, who keep around 3-5% of the amount transferred and then use a pay-platform or other anonymous form of sending money to send the money on to the real criminals. When the crimes are reported to the police, the only live trail leads directly to the money mules.

This means that everyone wins, except of course the victims and the money mules, who will be held as the only responsible party.

Report on Banker Trojans

Organized crime

Spam still represents a weak point for users in terms of preventing malware from entering their computers. Sometimes, the content itself of messages will be enough to make users suspicious.

However, there are often other indications such as spelling mistakes or incoherent information, which should warn users and prevent them from running files or clicking links.

In the case of messages with attachments, it is important that before opening them, users scan them with an antivirus solution to check if they contain malware.

Similarly, before clicking on any links in emails, you can place the cursor on the link to check if the link really points to the website that it claims to. Very often, links in these messages are camouflaged, and point to malicious addresses from which they download malware.

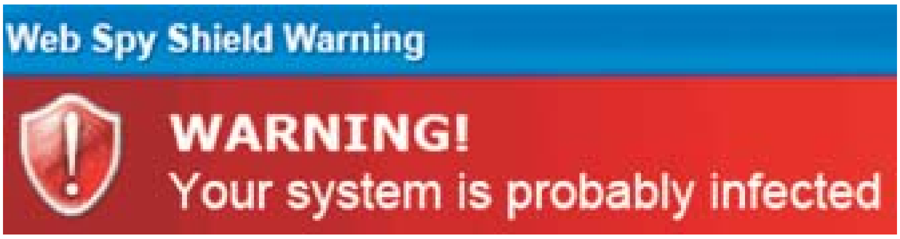
Criminals also infect legitimate web pages as a means for infecting users with banker Trojans. Be sure to keep systems fully up-to-date and patched to prevent any such malware exploiting vulnerabilities on your computers.

Rogue anti-malware programs in 2008

The last few months have witnessed the appearance of many false anti-malware programs, also known as rogue anti-malware. These types of programs are not new, but their high activity throughout the last six months has merited their inclusion in PandaLabs' yearly report.

Also, numerous spam messages have been found lately carrying these annoying programs. These messages use social engineering techniques to trick users by exploiting the latest news, controversial issues or celebrity videos.

Rogue anti-malware continuously displays alarming messages to exhaust the victim's patience and get them to register the product after paying the corresponding fee.



Web Spy Shield Warning

WARNING!
Your system is probably infected

Figure 15. False infection message.

Cyber-crooks take advantage of users' main concern about the Internet: theft of passwords, banking data or personal information. Therefore, there is no better way for criminals to achieve their objectives than to display messages that indicate the user's data is at risk as their computer has been infected by a password-stealing Trojan.

Therefore it is very important for users to learn to recognize these phony programs and avoid falling into the trap. Although many of these programs show interfaces and features very similar to those of real antiviruses, they are actually fake.

This article describes these programs, the usual infection vectors and how to respond to this threat. You can also see a series of graphs that show the significant growth of this type of malware that directly targets users' money.

Rogue anti-malware programs in 2008

Key features

Generally speaking, rogue anti-malware applications report a false infection on the computer and offer a solution to remove it. To do this, the user must register and pay a certain amount of money.

Although these tools are initially offered for 'free', users must pay to register. They offer free antivirus scans which are actually a fraud as they warn of non-existent threats or because those threats are actually installed by the tools themselves. They also display continuous, annoying messages claiming that the computer is infected.

After analyzing several examples of this type of malware, we can conclude they all behave in a similar way, not only with regard to the messages displayed but also to the changes they make to the system.

These are these programs' common traits:

- They display fake warning pop-ups, messages on the taskbar and change the screensaver.
- They look and pretend to work like a real antivirus.
- They complete scanning of the entire system very quickly.
- The infections they report refer to non-inexistent files on the affected system or files downloaded by the applications themselves.
- All of them ask users to pay a certain fee to register the product and disinfect the system.

As for the effects they have on computers, they make changes to the Windows Registry to trick the user into believing they are truly infected.

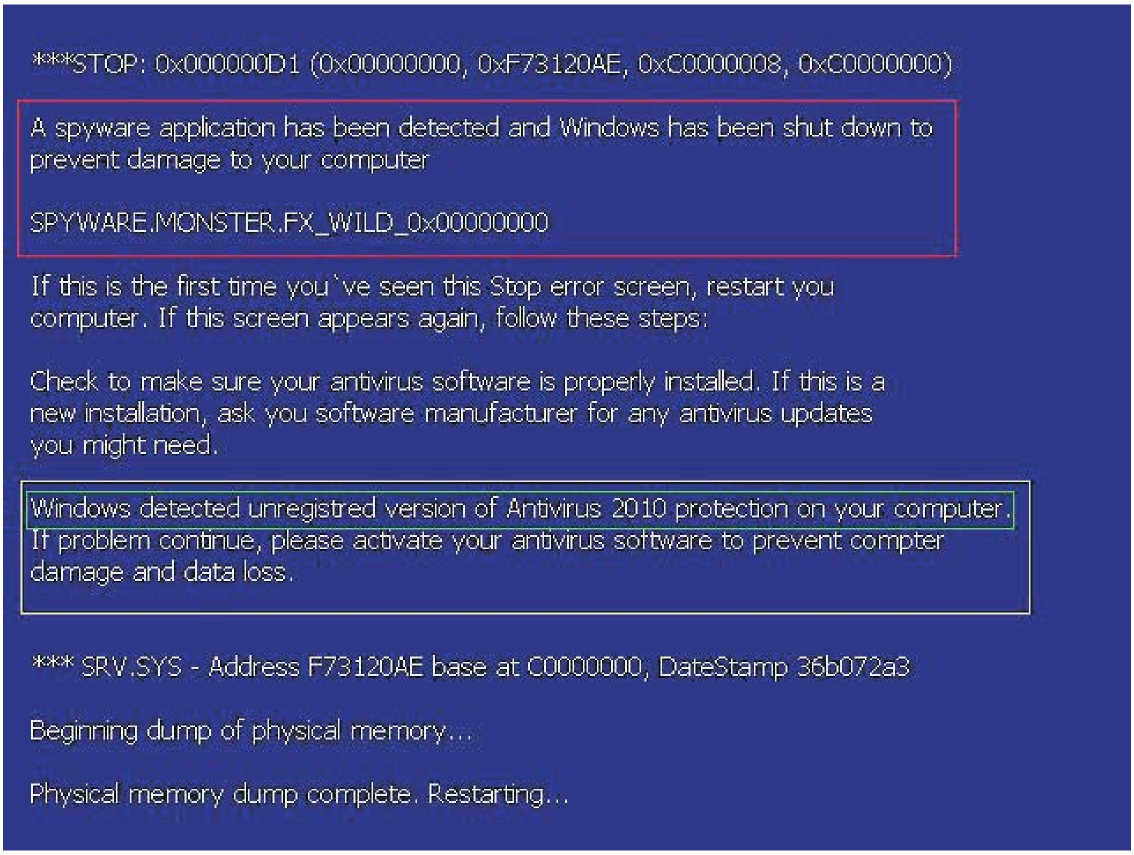
These changes have the following consequences:

- Modify the desktop theme.
- Establish a screensaver designed by the adware.
- Hide the Desktop and the Screen Saver tabs on the Display Properties screen. This way, users cannot modify the desktop theme or the screensaver.

Rogue anti-malware programs in 2008

Key features

Usually, the desktop theme and the screensaver established by the adware contain messages that warn the user that the computer is infected.



```
***STOP: 0x000000D1 (0x00000000, 0xF73120AE, 0xC0000008, 0xC0000000)

A spyware application has been detected and Windows has been shut down to
prevent damage to your computer

SPYWARE.MONSTER.FX_WILD_0x00000000

If this is the first time you`ve seen this Stop error screen, restart you
computer. If this screen appears again, follow these steps:

Check to make sure your antivirus software is properly installed. If this is a
new installation, ask you software manufacturer for any antivirus updates
you might need.

Windows detected unregistred version of Antivirus 2010 protection on your computer.
If problem continue, please activate your antivirus software to prevent compter
damage and data loss.

*** SRV.SYS - Address F73120AE base at C0000000, DateStamp 36b072a3

Beginning dump of physical memory...

Physical memory dump complete. Restarting...
```

Figure 16. A screensaver displayed by rogue AVs.

The purpose of these techniques is to exhaust the user’s patience so that they finally register the product and pay the corresponding fee. In the end, what seemed free is actually rather costly.

Rogue anti-malware programs in 2008

Key features

Many of these programs advertise themselves by claiming to detect more than other programs. The question is not that they detect more than the others, but that they detect non-inexistent threats or even threats the tools themselves have introduced on the computer. They exploit the myth that a security program that detects something others can't is a better product. That is, the more a security solution detects, the better. However, this couldn't be further from the truth; in this particular case, these solutions detect more simply because they detect false threats.

The purpose of these programs is purely economic: to get as many users as possible to buy the corresponding license.

The image below shows the different elements involved in the distribution of rogue AVs and the obtaining of users' personal data:

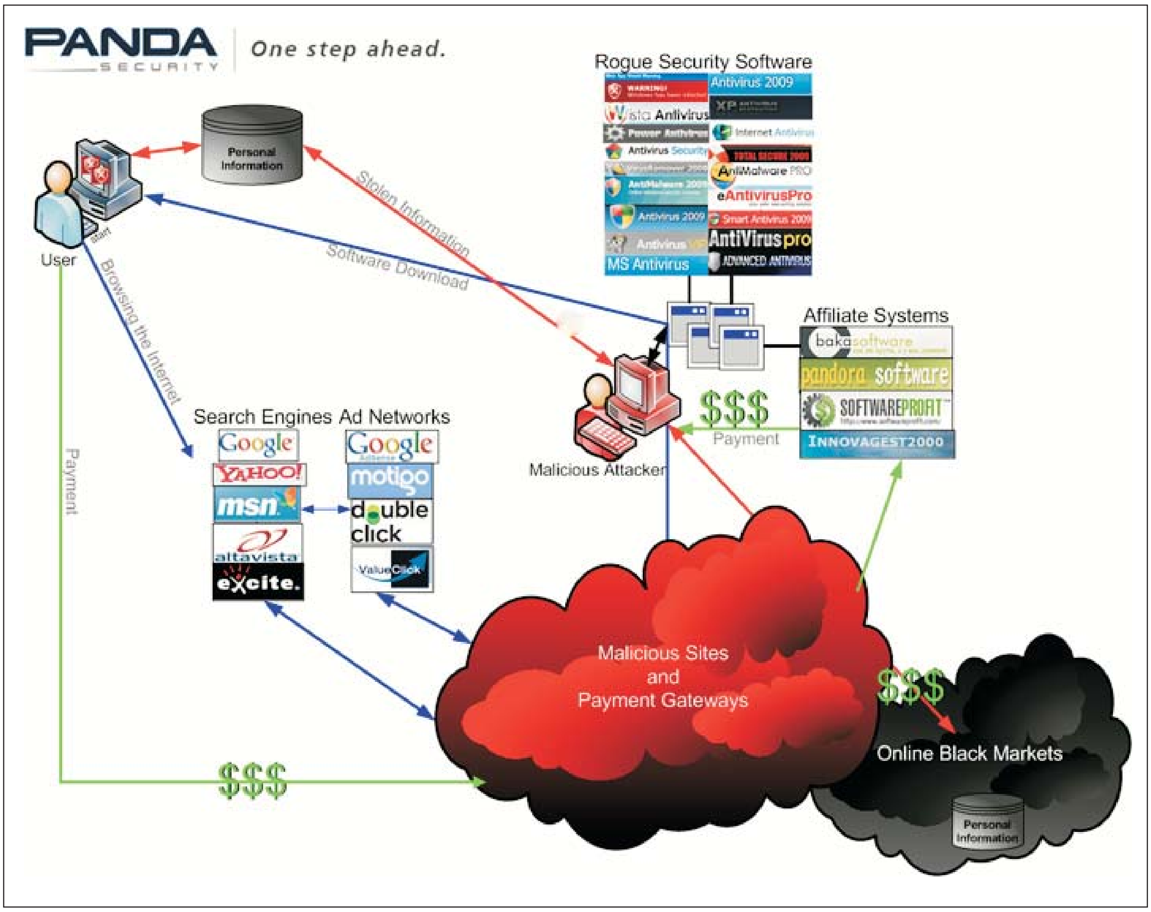


Figure 17. Distribution of rogue AVs.

Rogue anti-malware programs in 2008

Key features

Explanation:

- Step 1: The blue lines show the process by which a user is redirected to an infected Web page.
- Step 2: The red lines show the path the information collected follows from the user to the black market.
- Step 3: The green lines show payments made by users on malicious Web pages.

For more information, go to the PandaLabs blog.

Rogue anti-malware programs in 2008

Common infection vectors

One of the possible infection vectors is visits to web pages of dubious content, such as web pages with adult content. To do this, they use a technique known as Drive by download to download files. Through this technique, files can be automatically downloaded to computers without users' knowing by exploiting system flaws. They also use advertising banners that offer free downloads.

Another means of distribution is web pages offering pirate software. They use social engineering techniques to trick users as they rename files with attractive names to make users believe they are downloading cracks, serial numbers, etc.

However, cyber–crooks are aware of the profitability of this business and do everything they can to distribute these programs. Thus, not only can these programs be downloaded from pages of dubious reputation, but also from legitimate web pages. We published an article dealing with infections from legitimate pages back in July (Legitimate Webs in jeopardy).

Now, all is left to do is get users to visit these web pages; but, how? Through spam.

Some Trojan families like Exchanger and Spammer have been designed to send out spam messages massively.

This type of message includes the adware or contains a link to a web page where users inadvertently download the malicious file through the drive by download method above.

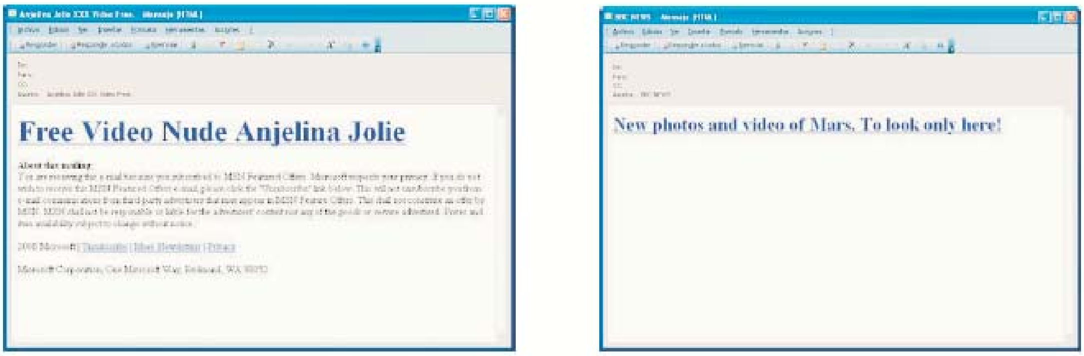
Spam messages are used to distribute all types of malware. However, in most cases they were used to spread Trojans, password-stealer Trojans more specifically. However, over the last few months we have detected a change in the type of malware distributed through spam.

Now, it is these false anti-malware programs that are top of the list. The main topics used to trick users continue to be the same: latest news and celebrity videos.

Rogue anti-malware programs in 2008

Common infection vectors

The following images show email messages used to distribute these programs:



Free Video Nude Anjelina Jolie

About this mailing:
You are receiving this e-mail because you subscribed to MSN Featured Offers. Microsoft respects your privacy. If you do not wish to receive the MSN Featured Offers e-mail, please click the "Unsubscribe" link below. This will not unsubscribe you from e-mail communications from third-party advertisers that may appear in MSN Feature Offers. This shall not constitute an offer by MSN. MSN shall not be responsible or liable for the advertisers' content nor any of the goods or service advertised. Prices and item availability subject to change without notice.

2008 Microsoft | Unsubscribe | More Newsletters | Privacy

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

New photos and video of Mars. To look only here!

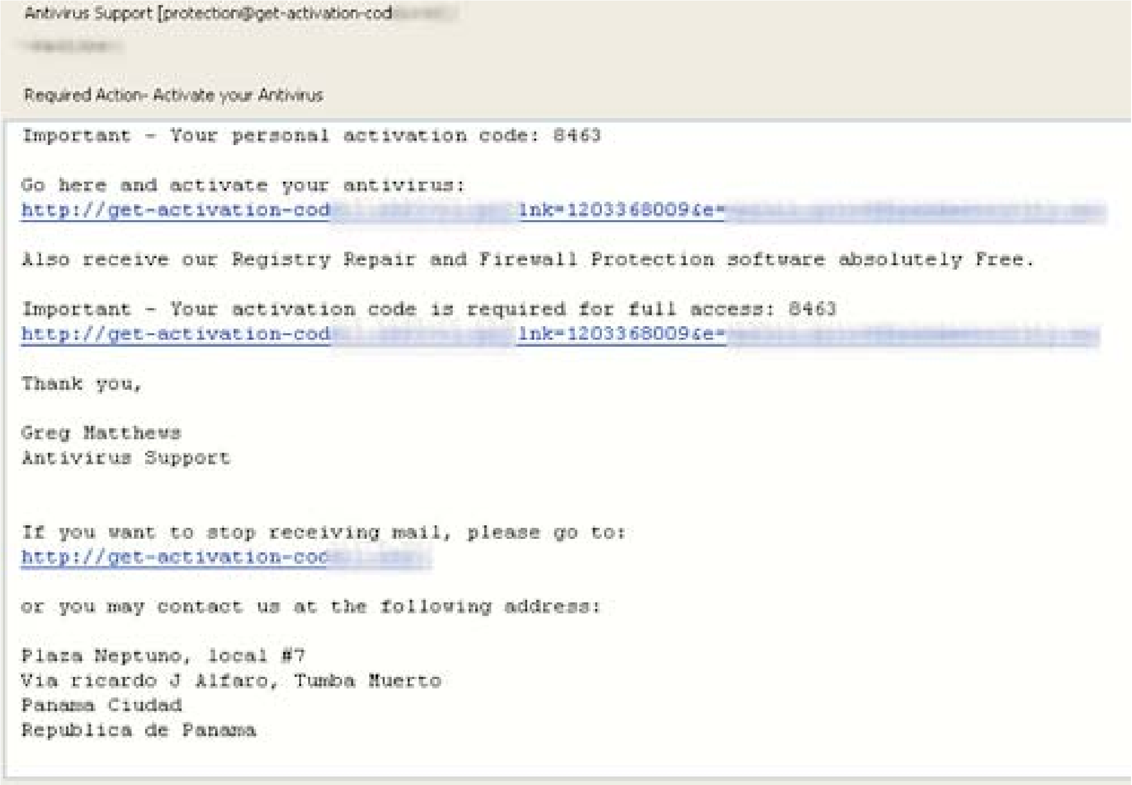
Figure 18. Spam messages to distribute Rogue AVs.

Finally, another common infection vector for these programs is malware. Some malware familes download this type of program. This is the case with Nuwar, or even some adware families that also download other adware strains, such as Adware/Bravesentry.

The latest social engineering techniques used by rogue antivirus distributors consist of skipping the infection warnings, etc. and directly sending an email to users telling them to activate their antivirus.

Rogue anti-malware programs in 2008

Common infection vectors



Antivirus Support [protection@get-activation-cod[redacted]

[redacted]

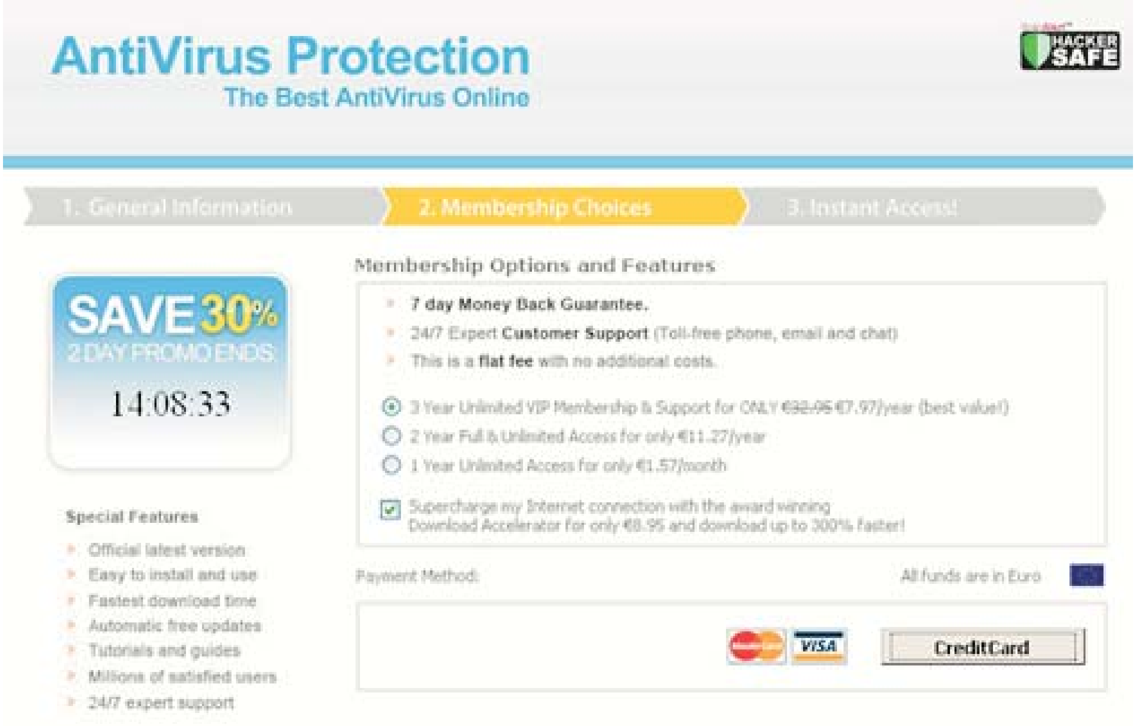
Required Action- Activate your Antivirus

```
Important - Your personal activation code: 8463

Go here and activate your antivirus:
http://get-activation-cod[redacted]lnk=1203368009&e=[redacted]

Also receive our Registry Repair and Firewall Protection software absolutely Free.

Important - Your activation code is required for full access: 8463
http://get-activation-cod[redacted]lnk=1203368009&e=[redacted]

Thank you,

Greg Matthews
Antivirus Support


If you want to stop receiving mail, please go to:
http://get-activation-coc[redacted]

or you may contact us at the following address:

Plaza Neptuno, local #7
Via ricardo J Alfaro, Tumba Muerto
Panama Ciudad
Republica de Panama
```

Figure 19. Spam message used to distribute rogue AVs.

Rogue anti-malware programs in 2008

Common infection vectors



AntiVirus Protection
The Best AntiVirus Online

1. General Information
2. Membership Choices
3. Instant Access!

SAVE 30%
2 DAY PROMO ENDS
14:08:33

Special Features

- Official latest version
- Easy to install and use
- Fastest download time
- Automatic free updates
- Tutorials and guides
- Millions of satisfied users
- 24/7 expert support

Membership Options and Features

- **7 day Money Back Guarantee.**
- 24/7 Expert **Customer Support** (Toll-free phone, email and chat)
- This is a **flat fee** with no additional costs.

● 3 Year Unlimited VIP Membership & Support for ONLY ~~€92.95~~ €7.97/year (best value!)
○ 2 Year Full & Unlimited Access for only €11.27/year
○ 1 Year Unlimited Access for only €1.57/month

☑ Supercharge my Internet connection with the award winning
Download Accelerator for only €8.95 and download up to 300% faster!

Payment Method:

All funds are in Euro

Figure 20. Rogue anti-malware registration page.

Rogue anti-malware programs in 2008

Figures

The third quarterly report already mentioned the significant increase in adware distribution, mainly due to these rogue anti-malware programs. As a result, according to the PandaLabs sensors, adware stood at 37.49% in Q3 instead of 22.03% (Q2).

The graph below shows the rogue AVs detected in 2008:

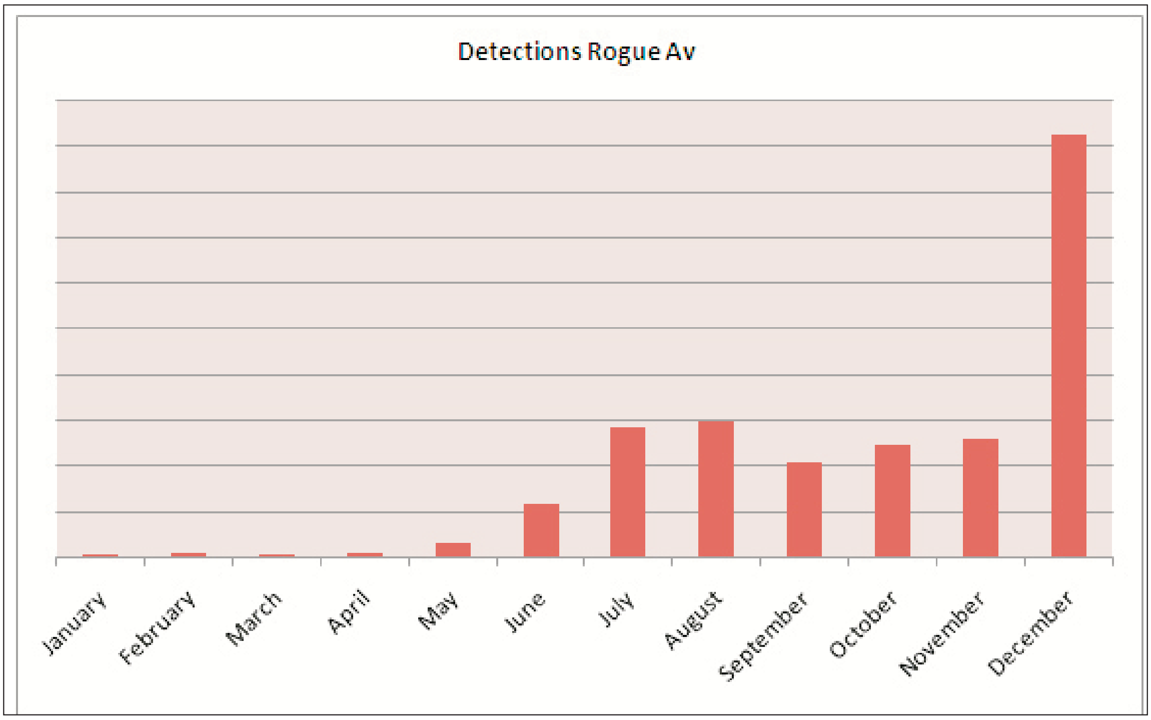


Figure 21. rogue AVs detected in 2008.

Rogue antiviruses began to rise in June and rocketed in December, tripling the August rogue antivirus figures (month with the highest 2008 detection ratios up until then).

Rogue anti-malware programs in 2008

Figures

What caused the December peak? The answer lies in the graph below:

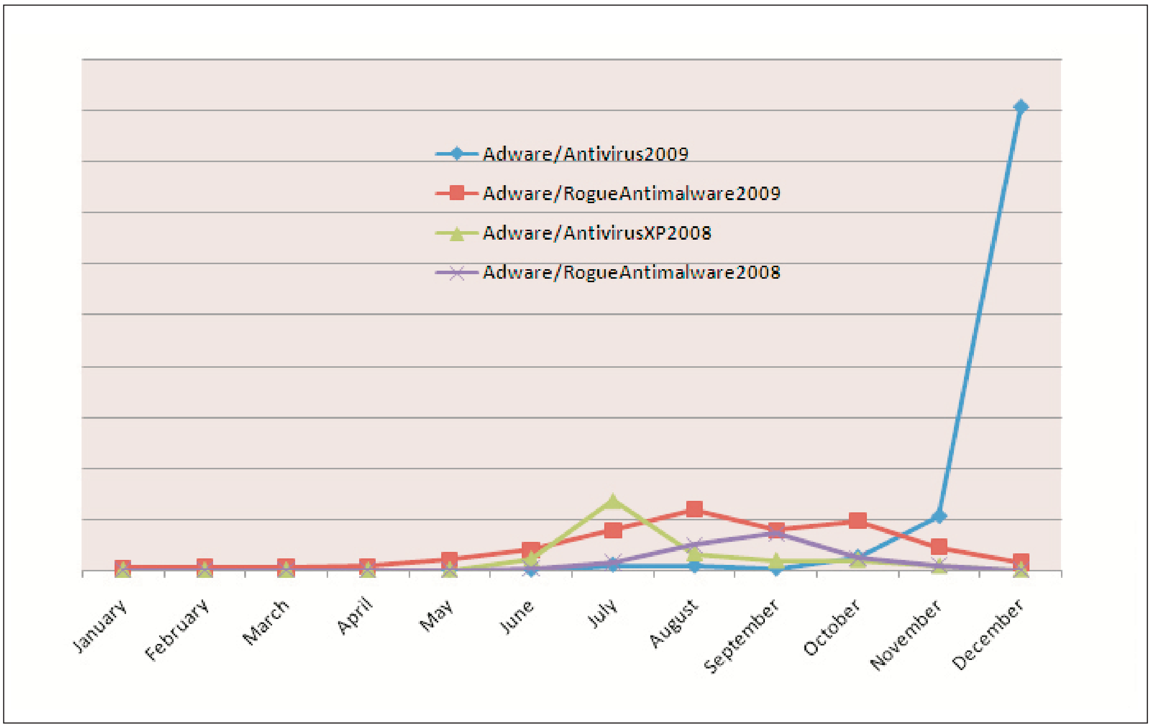


Figure 22. Most active rogue AVs in 2008.

The Adware/Antivirus2009 is responsible for this increase, as it is no doubt the most active rogue AV throughout 2008.

Rogue anti-malware programs in 2008

Figures

Below are different rogue AVs detected in 2008, and their percentages:

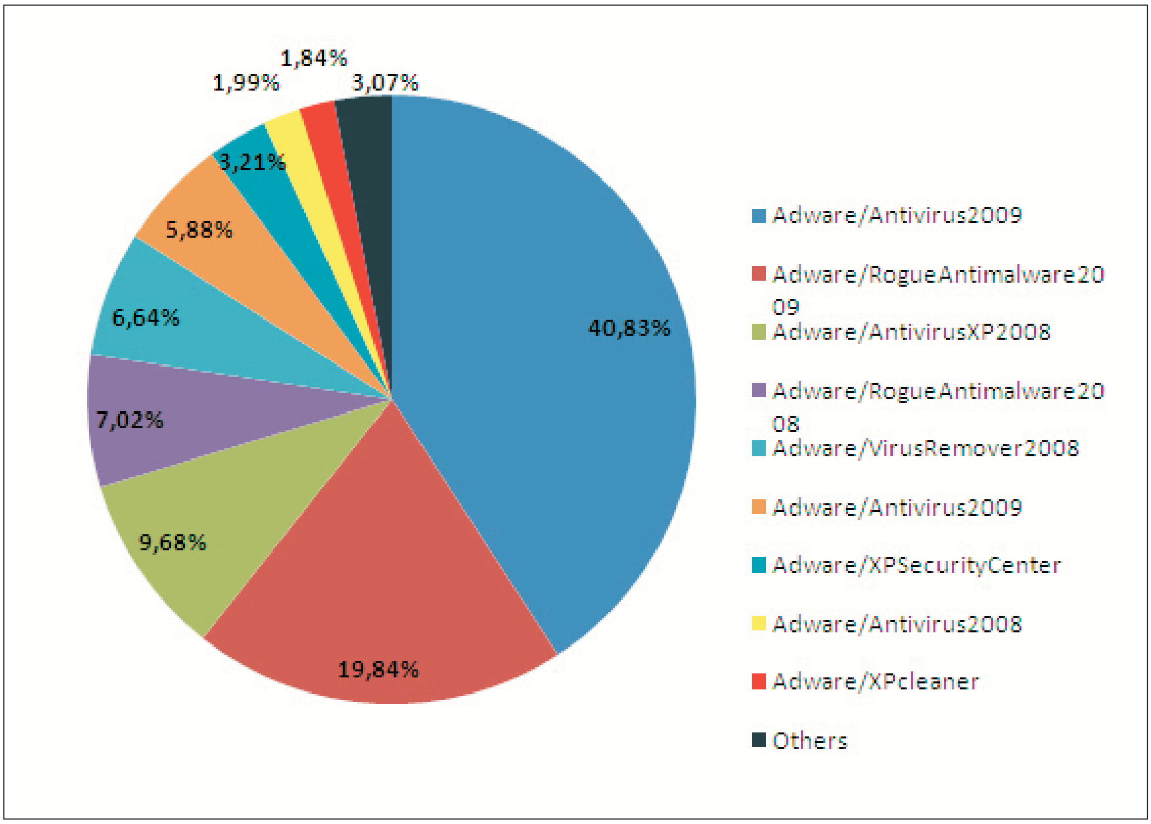


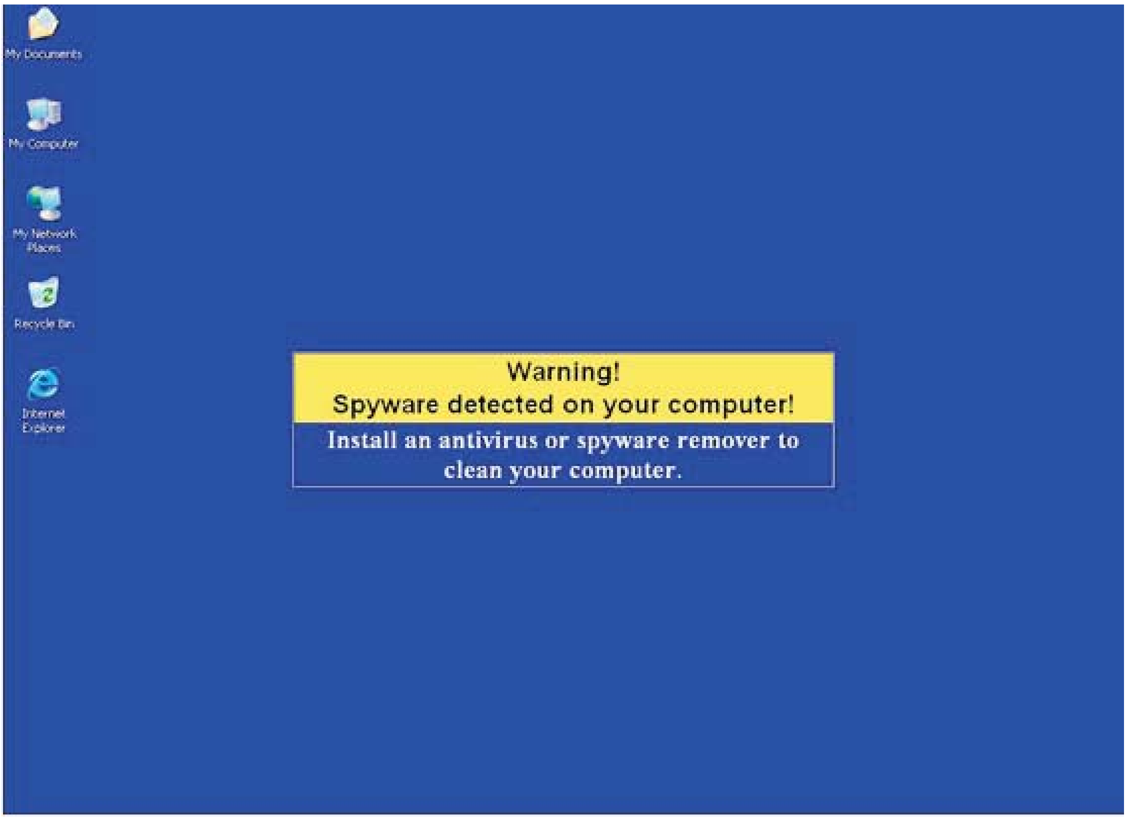
Figure 23. Rogue AVs detected in 2008.

Rogue anti-malware programs in 2008

MalwareProtector2008 in detail

As for the malware strains we have analyzed over these months, one really caught our attention due to the 'scary' screen saver it uses: a group of cockroaches eating up the desktop.

Once run, the adware replaces the desktop theme with the following:



Warning!
Spyware detected on your computer!
Install an antivirus or spyware remover to clean your computer.

Figure 24. Screensaver displayed by MalwareProtector2008.

Rogue anti-malware programs in 2008

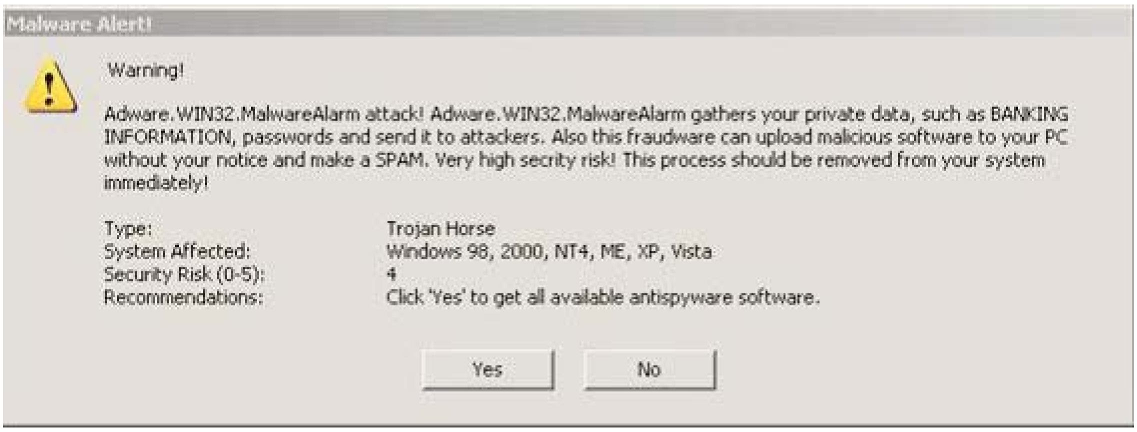
MalwareProtector2008 in detail

The message reads as follows:

Warning! Spyware detected on your computer! Install an antivirus or spyware remover to clean your computer.

This way, it tricks the user into believing their computer is infected.

Then, it shows a message warning users that their computer contains adware designed to steal passwords or banking data:



Malware Alert!

Warning!

Adware.WIN32.MalwareAlarm attack! Adware.WIN32.MalwareAlarm gathers your private data, such as BANKING INFORMATION, passwords and send it to attackers. Also this fraudware can upload malicious software to your PC without your notice and make a SPAM. Very high secrity risk! This process should be removed from your system immediately!

Type: Trojan Horse
System Affected: Windows 98, 2000, NT4, ME, XP, Vista
Security Risk (0-5): 4
Recommendations: Click 'Yes' to get all available antispyware software.

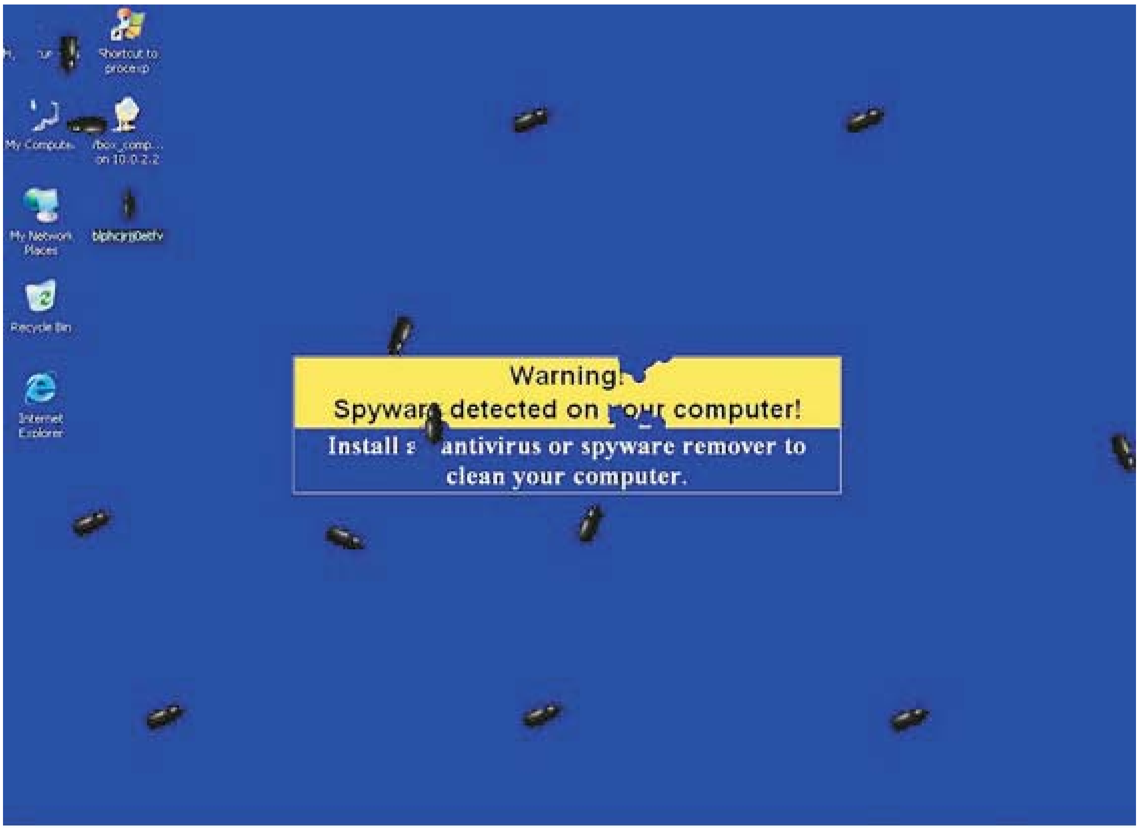
Figure 25. Warning message displayed by MalwareProtector2008.

Rogue anti-malware programs in 2008

MalwareProtector2008 in detail

Also, users are prompted to remove the threat from the system as soon as possible. To do so, they are offered an anti-spyware program to disinfect the computer.

If the user selects 'No' a screensaver runs from time to time showing a group of cockroaches eating up the desktop:



Warning!
Spyware detected on your computer!
Install a antivirus or spyware remover to clean your computer.

Figure 26. Screensaver displayed by MalwareProtector2008.

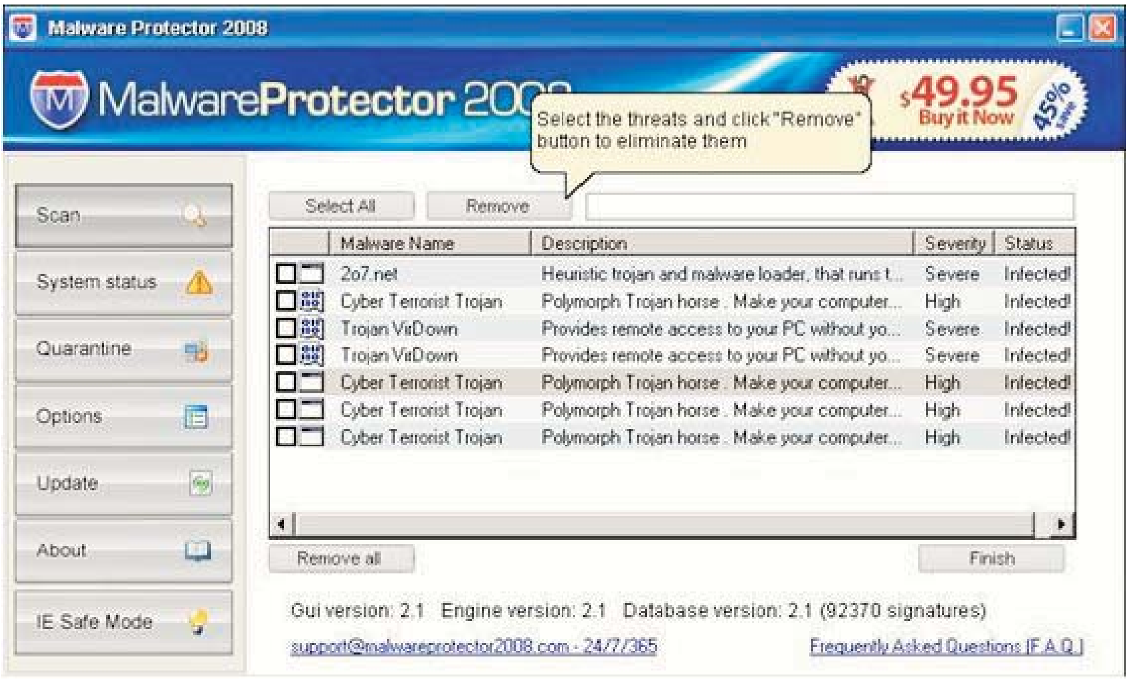
Rogue anti-malware programs in 2008

MalwareProtector2008 in detail

This is another technique used to get the affected user to accept the message and download a false antivirus program.

If the user accepts the message, the false anti-malware program will start to download. Once downloaded, the program starts scanning the system for possible malware.

However, the scan result is a complete fraud and shows a series of non-existent threats that have supposedly infected the computer:



Select the threats and click "Remove" button to eliminate them

	Malware Name	Description	Severity	Status
□	2o7.net	Heuristic trojan and malware loader, that runs t...	Severe	Infected!
□	Cyber Terrorist Trojan	Polymorph Trojan horse . Make your computer...	High	Infected!
□	Trojan VirDown	Provides remote access to your PC without yo...	Severe	Infected!
□	Trojan VirDown	Provides remote access to your PC without yo...	Severe	Infected!
□	Cyber Terrorist Trojan	Polymorph Trojan horse . Make your computer...	High	Infected!
□	Cyber Terrorist Trojan	Polymorph Trojan horse . Make your computer...	High	Infected!
□	Cyber Terrorist Trojan	Polymorph Trojan horse . Make your computer...	High	Infected!

Gui version: 2.1 Engine version: 2.1 Database version: 2.1 (92370 signatures)

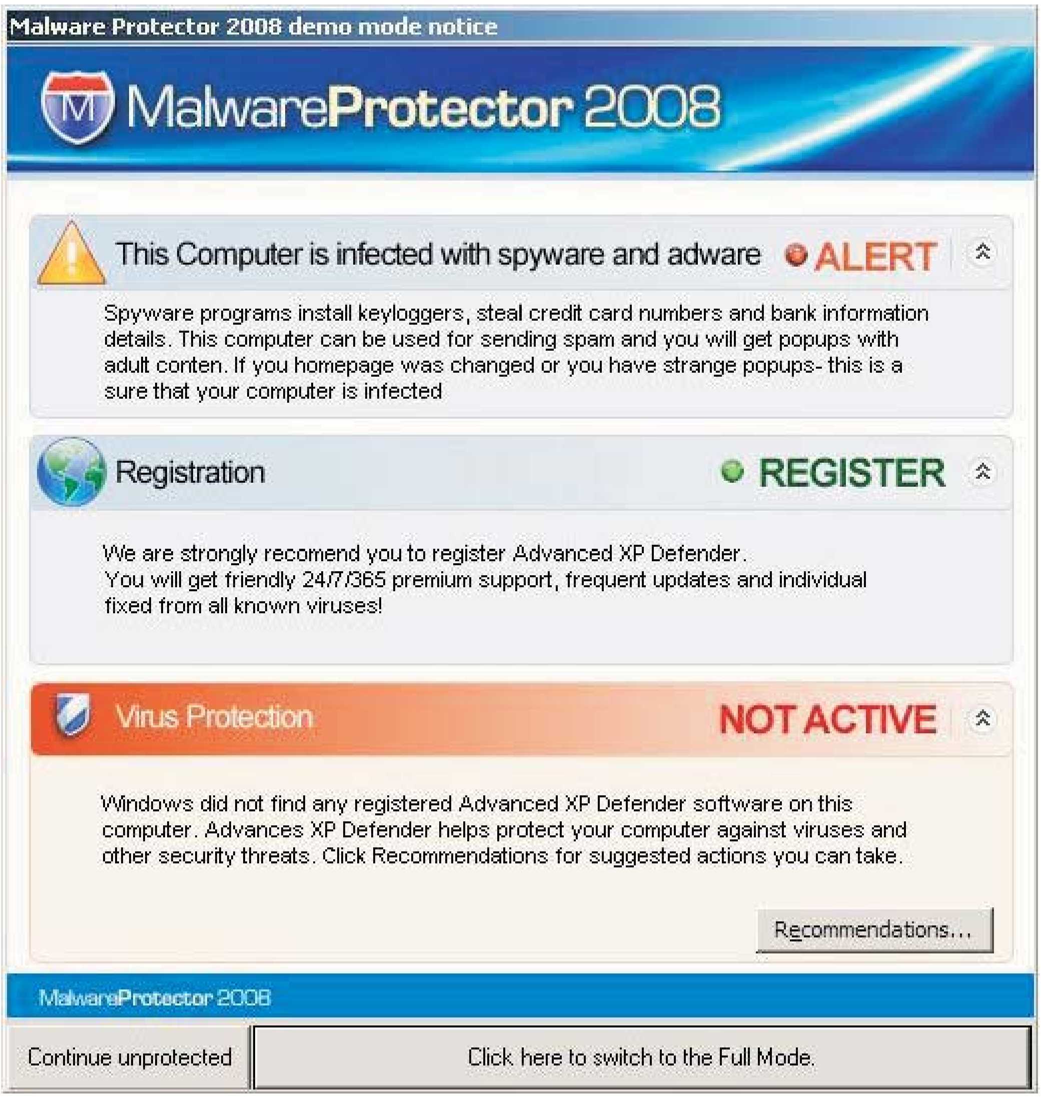
support@malwareprotector2008.com - 24/7/365 Frequently Asked Questions [F.A.Q.]

Figure 27. MalwareProtector2008 scan results.

Rogue anti-malware programs in 2008

MalwareProtector2008 in detail

If the user selects the option to remove malware, a screen is displayed informing that the computer is infected with adware and spyware. They are also encouraged to register to remove these threats and stay protected:



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

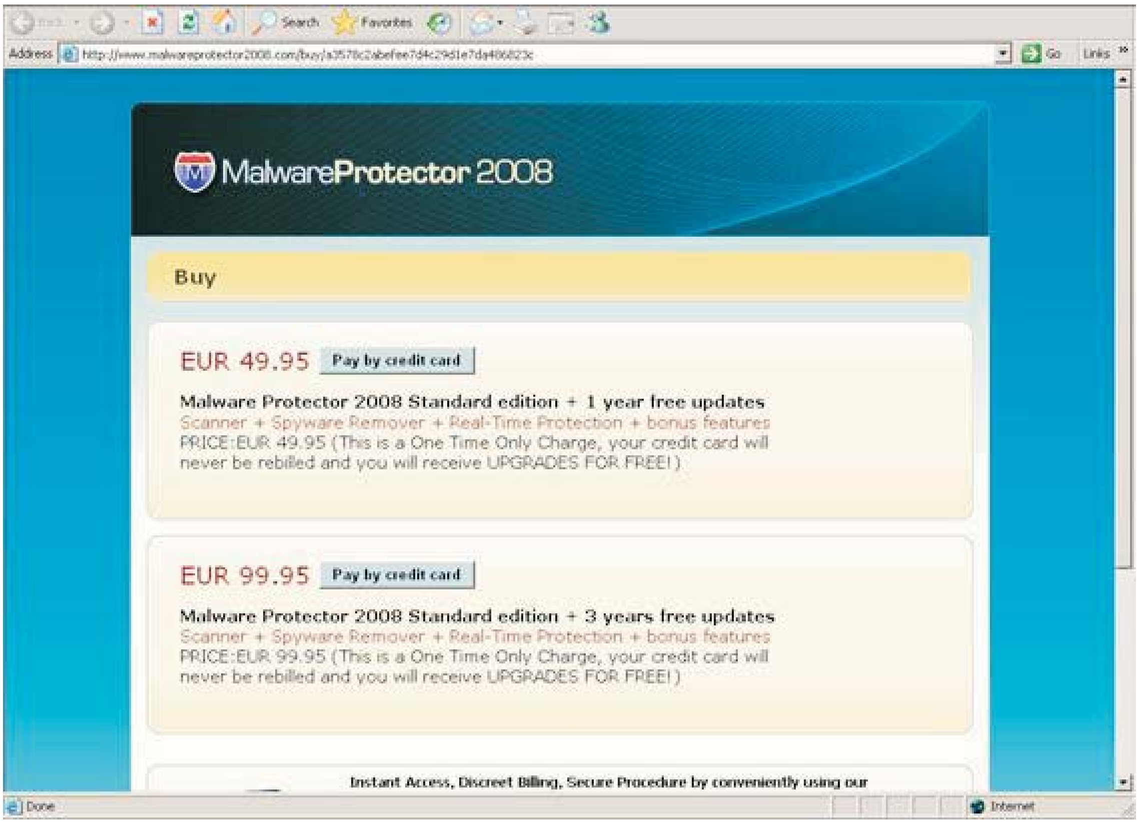
Windows did not find any registered Advanced XP Defender software on this computer. Advances XP Defender helps protect your computer against viruses and other security threats. Click Recommendations for suggested actions you can take.

Figure 28. MalwareProtector2008 interface.

Rogue anti-malware programs in 2008

MalwareProtector2008 in detail

To register, the user has to pay the price indicated on the website they are taken to after clicking the button to get the full version:



http://www.malwareprotector2008.com/buy/a3578c2abefee7d4c29d1e7da486823c

MalwareProtector 2008

Buy

EUR 49.95 Pay by credit card

Malware Protector 2008 Standard edition + 1 year free updates
Scanner + Spyware Remover + Real-Time Protection + bonus features
PRICE:EUR 49.95 (This is a One Time Only Charge, your credit card will never be rebilled and you will receive UPGRADES FOR FREE!)

EUR 99.95 Pay by credit card

Malware Protector 2008 Standard edition + 3 years free updates
Scanner + Spyware Remover + Real-Time Protection + bonus features
PRICE:EUR 99.95 (This is a One Time Only Charge, your credit card will never be rebilled and you will receive UPGRADES FOR FREE!)

Instant Access, Discreet Billing, Secure Procedure by conveniently using our

Figure 29. MalwareProtector2008 Web page.

However, even though you have registered and paid the corresponding fee, the computer will still be unprotected and vulnerable to all types of threats.

This adware's characteristics are very similar to those of other rogue anti-malware: the messages displayed, the application interface, the way it works… We hope this in-depth analysis will allow users to identify this type of program.

Rogue anti-malware programs in 2008

Tips

Spam is the usual means of propagation for this type of program. Be extremely careful with any email message you receive with eye-catching news stories or subjects. These emails typically invite users to click a link to watch a video or images of some false news stories. Don't click on links included in these messages, as you might be downloading one of these rogue anti-malware programs into your computer.

Be wary of programs you don't remember installing and which start showing false infection warnings or pop-ups that encourage you to buy some kind of antivirus software. Most probably, one of these malicious programs has installed on your computer.
Keep all programs up-to-date as many malicious codes exploit vulnerabilities on computers to infect them.

Scan your computer regularly with a reliable antivirus, so that if any of these codes is hiding on the computer, it can be detected and removed.

Rogue AVs have become the leading malware this year, and have provided their creators a lucrative source of income. December has been their most active month, tripling the number of detections of its predecessor. We believe we will observe a similar trend at the beginning of 2009. We hope we are wrong!

Malware Trends in 2008

Fake antiviruses are one of the trends that have grown most during 2008. A fake antivirus is a type of adware that passes itself off as a security solution and, on running on the computer, makes users believe they are infected with dozens of malware strains to try and sell them an antivirus to fix the false problem. Their aim is to obtain financial benefits from infections, and according to our data, cyber-crooks could be making more than ten million euros every month.

Also, our research has shown that the financial crisis undergone by several countries worldwide has become a weapon for cyber-crooks. In 2008 the number of new malware samples in circulation has risen with every stock market crash. Similarly, the increase in the unemployment rate has translated into a boom in spam, especially spam related to job offers aimed at recruiting money mules (people that move money obtained from illegal activities from one account to another to launder it).

Cyber-crooks take advantage of people's dire economic situation to dupe them with tempting offers. On some occasions, these offers consist of false mortgage loans, etc. to obtain users' banking data.

Due to their increasing popularity, social networks have become one of the most popular means used by cyber-crooks to distribute their creations.

The use of both legitimate and malicious pages (via SQL injection attacks) has been one of the rising trends in 2008.

The use of boot viruses (which replace the computers' original Master Boot Record with virus code) to hide Trojans was another new technique in 2008, and will continue to rise next year. This is a very old technique which became highly popular at the beginning of the 90s but had practically disappeared in recent years, until now. During 2009 we will probably see this and other old techniques that can still be extremely effective for hiding malware.

The huge rise in malware, as predicted in 2007, has been one of the year's highlights. With an average of 22,000 samples received everyday day at our laboratory, between January and August 2008 we detected more malware than in the previous 17 years combined. This shows an impressive increase in new threats, which many users seem unaware of.

We expect these figures will continue to rise in 2009. As for methods of malware distribution, social networks will be further exploited, not only by worms that spread from some users to others, but by malicious codes designed to take more dangerous actions like theft of confidential data. Similarly, malware distribution via SQL injection attacks will continue to grow.

A technique that will certainly become popular in 2009 will be the use of customized packers and obfuscators. Cyber-criminals will try to avoid the standard tools available in forums, websites, etc., and turn to their own obfuscators in an attempt to hide malicious code and evade 'signature-based' detection by security solutions.

Malware Trends in 2008

The same reason can explain the rebirth of classic malicious code such as viruses expected in 2009. The use of increasingly sophisticated detection technologies like Panda Security's Collective Intelligence, capable of detecting even low-level attacks and the newest malware techniques, will make cyber-crooks turn to old codes, adapted to new needs. Forget about viruses designed to prevent systems from working or files from being opened, as they did ten years ago, and get ready for viruses aimed at hiding Trojans used for theft of banking information.

Finally, we'd like to mention one of this year's most important initiatives: the creation of AMTSO (AntiMalware Testing Standards Organization). The group was officially born in an event organized by Panda in Bilbao (Spain), which served to establish the principles of the organization. Further meetings took place throughout 2008: in Holland (hosted by Norman), in Seattle (hosted by Microsoft) and in Oxford (hosted by Sophos). During this last meeting, we finished two documents we had been working on all year.

One of them was "Fundamental Principles of Testing", which includes recommendations on how to test anti-malware solutions (to be applied by testers, editors and manufacturers).

The other was "Best Practices for Dynamic Testing", which includes best practices on how to test the efficiency of anti-malware products in real attack situations.

We have already planned the next two meetings to take place in 2009: at the beginning of February we will meet in Mountain View (USA) to work on a series of new documents we are currently preparing. This meeting will be organized by Symantec. In May we will meet in Budapest, in an event organized by VirusBuster.

The two documents mentioned above can be downloaded from the AMTSO website (www.amtso.org), where you will also find news regarding this organization.

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/