



PandaLabs

Annual Report 2006





Index

Introduction	4
A Brief Overview of the Fourth Quarter	7
October	7
November	8
December	9
Fourth Quarter Figures	11
Distribution of New Threats Detected	11
Threats Detected by Panda ActiveScan	12
Malware in Trustworthy Sources	13
Trojans in MP3 Players	13
Malware on Video iPods.....	14
A Wikipedia Trojan Courtesy	15
Google and the Revenge of the Kamasutra Worm	16
Conclusions.....	16
Virtual Presence Attacks	17
Second Life: On Rings and Viscous Substances.....	17
MySpace: A New Attack to Add to the List.....	18
Conclusions.....	19
Alarm over the Skype Worm	20
Skype: The Popularity of IP Telephone	20
Skype Worm: First Contact.....	20
The Smoke Clears	21
Conclusions.....	21
A Christmas Story	22
Social Engineering	22
The Spirit of Christmas Past	23
The Spirit of Christmas Present	24
Conclusions	26



2006 in Perspective	27
Distribution of New Threats Detected throughout the Year	27
Threats Detected by Panda ActiveScan during 2006	29
Evolution of Malware Categories in 2006	31
What Can We Expect from 2007?	33
New Threats	34
About PandaLabs	36



Introduction

This report will analyze the most significant malware related events that occurred in 2006. It will focus on changes that have developed, and it will attempt to point out possible tendencies to be expected throughout 2007.

Tendencies encountered in 2006 were consistent with those of the previous years in regards to the appearance of new malware. The number and diversity of the varieties coming on the scene shed light on the magnitude of problem being confronted.

Nonetheless, it is important to remember that one of the occurrences of 2006 was that massive infections were mitigated in such a way that they continually generated less news in the press. This has two consequences: a false sense of security, resulting from the fact that users may have the impression that there is no malware in circulation, or that since it is not making the news, it poses no threat.

However, that is not the case. The shift in tendency of malware creation and distribution marks a change in strategy, and this new strategy has come to be known as the "silent epidemic". During 2006, the trend of new malware appearing held its course, and it should not be forgotten that in 2005 more malware appeared than in Panda's previous 15 years. How can this message be transmitted to public opinion without creating a state of alarm?

Spam continues to be a problem, and the evolution of antispam filters only mitigates the problem. Spammers that have economic resources develop increasingly elaborate techniques for distributing their spam.

The significant increase of adware infections can be credited to the fact that users do not feel adware is as dangerous as viruses, worms or Trojans. Nonetheless, many of these installations, some of which even have EULAs, lead to the installation of multiple programs for which the end user has not given express consent.

The development and implementation of increasingly complex code packers obscures the code in an attempt to further complicate the work of antimalware laboratories.

The entry of the mafia and the corresponding economic resources has given malware creators the capacity not only to create but also to acquire tools that complement their arsenal. Phishing attack creation kits, bot network rental kits, make-to-order Trojan creation services, exploits sales, vulnerabilities and more have come on the scene, maturing a black market that is said to move more money than the whole antimalware industry.

Throughout 2006, we have been attentive to the publication of zero-day exploits on a large number of operating systems, browsers and applications. Many of these exploits were not patched by the manufacturers for a period of weeks. What's more, in order to increase the time between patching, a trend has been observed to publish exploits the day after the Microsoft patch publication cycle.



We have also begun to observe that standard functionalities, which are initially not offensive, have become new vectors of attack. We remember the cases of the .mov format, and the more recent cases of the Adobe .pdf files in which the use of an extended functionality permitted the execution of malicious code. The additional problem to these cases is that they do not deal with vulnerabilities, so the solution is more complex, above all when it is taken into consideration that these products are in mass use.

The market race giving priority to incorporating extended functionalities brings us to ever increasing levels of complexity that end up negatively affecting security. Thus, it is necessary for the industry to take a moment and reflect on the problems resulting when priority is not given to security as a parameter intrinsic to any system.

The use of traditional methods, such as social engineering, makes it clear that we have a long way to go in educating users. Worms that propagate during Christmas, Valentine's Day, etc. continue to exist and reveal that users are still not completely aware of the risks implied by running just any old application on their computers. It is true that great progress has been made since the massive epidemics of old no longer occur. Accordingly, if more efficient tools are available for combat, and if user awareness is heightened, it will be possible to reduce these even more.



A Brief Overview of the Fourth Quarter

October

- Day 1.** SANS raised its level of alert to Yellow due to the vulnerability in the WebViewFolderIcon.
- Day 2.** There is continued concern over the vulnerability of the setSlice method of the WebViewFolderIcon. eEye launches a zero-day vulnerability warning.
- Day 3.** Spiegelmock and Wbeelsoi confess that their grave failure in Firefox, presented on Toorcon, was only a joke to get attention.
- Day 5.** Google Code Search launches to help developers easily find source code on the Internet. At the same time it is unveiled as a tool to locate objectives affected by specific vulnerabilities.
- Day 7.** Microsoft revokes the MVP (Microsoft Valuable Professional) title from Cyril Paciullo, creator of Messenger Plus!, after a multitude of complaints in regards to his implication in the distribution of aggressive adware.
- Day 8.** The Google blog was attacked over the weekend, including a false entry announcing the cancellation of the Click-to-call project.
- Day 10.** Second Tuesday of the month: Regular cycle for Microsoft security bulletins. Microsoft experiences problems in the automatic distribution of its security patches. Browser market shares are published: Internet Explorer (82.1%), Firefox (12.46%). Firefox keeps clawing for market share.
- Day 11.** McDonalds Japan exposes 10,000 of its customers to a Trojan spy by way of a gift MP3.
- Day 12.** Web page caching by ISPs leads to security problems by distributing malware after the original pages were pulled down. Microsoft warns of the existence of proof-of-concept code that exploits vulnerabilities in PowerPoint 2003. Researchers discover a site that imitates Google Italy and that installs malware on its visitors' computers.
- Day 13.** The installation of Internet Explorer 7 can be considered as a malicious act by some antivirus programs.
- Day 15.** The existence of a proof-of-concept is discovered, which makes it possible to take control of a Linux system via a vulnerability in the NVidia drivers.
- Day 16.** A vulnerability in information dissemination is discovered in Internet Explorer 7 just hours after its launch.
- Day 17.** Apple admits to the existence of a shipment of Video iPods that includes serial malware and blames Windows for the failure.
- Day 18.** Discussion is engaged between Microsoft and investigators as to whether the Internet Explorer 7 failure is due to the browser or is really due to Outlook Express.
- Day 20.** A Trojan variant is discovered that installs antivirus software to eliminate other possible competitors from computers it affects.
- Day 24.** A failure, which can be taken advantage of to disguise falsified websites (phishing) is discovered in Internet Explorer 7. A breach of security is confirmed in the Los Alamos nuclear weapons laboratory.
- Day 26.** A security firm finds a way to dodge the Windows Patch Guard protection for 64 bit processors.
- Day 27.** US senator Edward Markey is successful in launching a warrant of arrest against researcher, Christopher Soghoian, who created a webpage to produce false boarding passes. The largest bot network of the last two years is discovered: one million zombies.



- Day 29.** A study is published, which expounds on the different “surprises” found in the Windows Vista End User License.
Three USB keys, with classified information from Los Alamos laboratory, are discovered in a registration in relation to a drug-trafficking case.
Senator Edward Markey defends researcher Christopher Soghoian after being informed on the intentions of his study.
- Day 30.** The existence of an error, which had been corrected in a previous version, was discovered in Firefox 2.0.
Code capable of disabling the Windows XP firewall is published.
- Day 31.** The popularity of video codecs is confirmed as a medium for distributing malware.
The Nuwar.A worm, which spreads in email messages that warn the readers of the beginning of the Third World War, is detected.

November

- Day 1.** H.D. Moore, responsible for the Month of Browser bugs, publishes code that is capable of exploiting a vulnerability in Apple Macintosh computers' WiFi drivers.
Window CE v6 is launched.
- Day 2.** Breaking news is published on an agreement between Microsoft and Novell.
- Day 3.** A new malware proof-of-concept, which affects the Mac OS X operating system, is published.
- Day 6.** A new vulnerability is discovered in Windows XML Core Services.
It has to do with the existence, in the German Wikipedia, of a page that distributes Trojans under the false impression of being a Microsoft patch for the Bagle worm (2003).
- Day 7.** Four arrests made in Chile for an IT attack against various entities including NASA.
An iDefense article affirms that the antivirus companies were not capable of detecting the secondary effects of the Spamta (pharmaceutical related spam) worms.
Google accidentally sends the Tearec.A worm to 50,000 subscribers on the Google Video list.
- Day 8.** In some telephone statements, James Allchin, former co-president of Microsoft, suggests that Windows Vista will not need antivirus software.
- Day 9.** After contracting Mark Russinovich, Microsoft publishes the tools created by the expert on its webpage. Among these is one that detects the controversial Sony rootkit (XCP).
- Day 10.** Authentium refutes the declarations made in the iDefense article, revealing that they silently alerted various government agencies as to its effects.
- Day 13.** James Allchin declares that his statements on Windows Vista and the use of antivirus software were taken out of context and misinterpreted.
Windows Live OneCare security software gives a false positive, detecting the Gmail web mail service as a virus (BAT/BWG.A).
- Day 15.** Four arrests were made in Spain (two of which were minors) for implications in identity theft and blackmail, using web cameras.
- Day 16.** In Chile, two of those accused of illegally penetrating the NASA servers and those of other US government agencies were set free. They were prohibited access to computers.
Steve Ballmer, Microsoft CEO, affirms that Linux illegally uses Microsoft's intellectual property.
Code, similar to that used by the Zotob worm, which exploits a critical vulnerability in Windows 2000, is published.
- Day 18.** A man is put on trial in England for illegally accessing ATMs, using an MP3 player.
- Day 21.** A worm detected in the virtual world of Second Life copies a multitude of spinning golden rings, slowing down the game experience.
- Day 23.** Microsoft begins legal action against different phishers, resulting in 129 different accusations and at least one conviction in Turkey.



- Day 24.** A proof-of-concept is created for Mac OS X: an adware model.
- Day 27.** A vulnerability is detected in Firefox, which can lead to the disclosure of passwords for diverse websites.
According to one study, Spam accounts for 90% of the email messages in circulation.
- Day 30.** Windows Vista is launched for the business World. The domestic user version will be launched on January 30th of 2007.

December

- Day 1.** A critical vulnerability, which can be exploited when a PDF file is opened via Internet Explorer, is detected in Adobe Reader and Adobe Acrobat.
EveryDNS begins to suffer a Distributor Service Denial attack, which is able to affect thousands of sites, including OpenDNS.
- Day 2.** A worm, which uses a QuickTime characteristic to compromise the MySpace profile access information and distribute adware (Zango), is detected in MySpace
- Day 5.** MySpace.com requests Apple Computer to update QuickTime in an effort to stop the expansion of the worm.
According to FBI figures, cybercrime in 2005 accounted for losses on the scale of 62 million dollars, while the antimalware solutions market reported earnings of 26 million dollars.
Microsoft publishes a security warning to notify of a vulnerability in Word that permits code to be executed upon opening a malicious Word document. The vulnerability also affects the version of Word used on MAC systems.
- Day 6.** A Romanian hacker is convicted for compromising 150 computers owned by NASA, the Department of Energy and the US Navy.
A Trojan appears, which is passed off as a Windows Vista crack.
- Day 7.** The first example of malware for Symbian based mobile telephones is detected; the malware seeks to spy on the user, making the leap from simply destroying data to actually using malware to extract the user's confidential information.
Adobe urges users to install the security update for the vulnerability in Adobe Acrobat and Adobe Reader version 7.
A vulnerability is detected in Windows Media Player.
- Day 8.** A program appears, which supposedly permits faking the Windows Vista validation process, allowing illegal copies to be used.
- Day 11.** A new vulnerability is discovered in Word. In the corresponding security warning, Microsoft confirms that it is being used on a limited basis for highly directed attacks.
- Day 12.** Second Tuesday of December: 7 Microsoft security bulletins.
The University of Los Angeles, in California, admits that the personal information of 800,000 current and former students has been compromised.
- Day 13.** A new version of ransomware is discovered, this malware compromises email accounts and does not allow the rightful user to gain access until paying a determined fee.
A court convicts an ex-systems administrator for installing a logical bomb in his former company's computer network and seeking to earn money from its collapse in the Stock Market.
- Day 14.** A new vulnerability is found in Microsoft Word (the third in less than one month).
- Day 15.** Yahoo! launches a "highly critical" security update for the company's instant messaging program: Yahoo! Messenger.
Only a few hours later, it is confirmed that said update modifies the user's Yahoo Mail options.
According to one antivirus company, there is a Windows Vista vulnerability on the black market, on sale for 50,000 dollars.



- Day 18.** Great commotion is caused over the possible appearance of a worm, which propagates by way of a Skype vulnerability.
- Day 20.** A "Month of Apple Bugs" is announced for January 2007.
A Microsoft Zune player, sold in a Chicago based Wal-Mart, contained a nearly two-hour-long video of a homosexual orgy.
- Day 22.** Microsoft publicly admits to the existence of a vulnerability in the Windows Vista Client/Server Runtime Server.
- Day 27.** The malware Christmas season begins with the appearance of Christmas worms.
New vulnerabilities appear in PowerPoint.
- Day 29.** Ford Motor Company will launch automobiles with Microsoft's Sync operating systems. In 2008 this is expected to be an optional characteristic.

Fourth Quarter Figures

Distribution of New Threats Detected

The following pie chart shows the distribution of new variations of malware types, detected by PandaLabs during the last quarter of 2006:

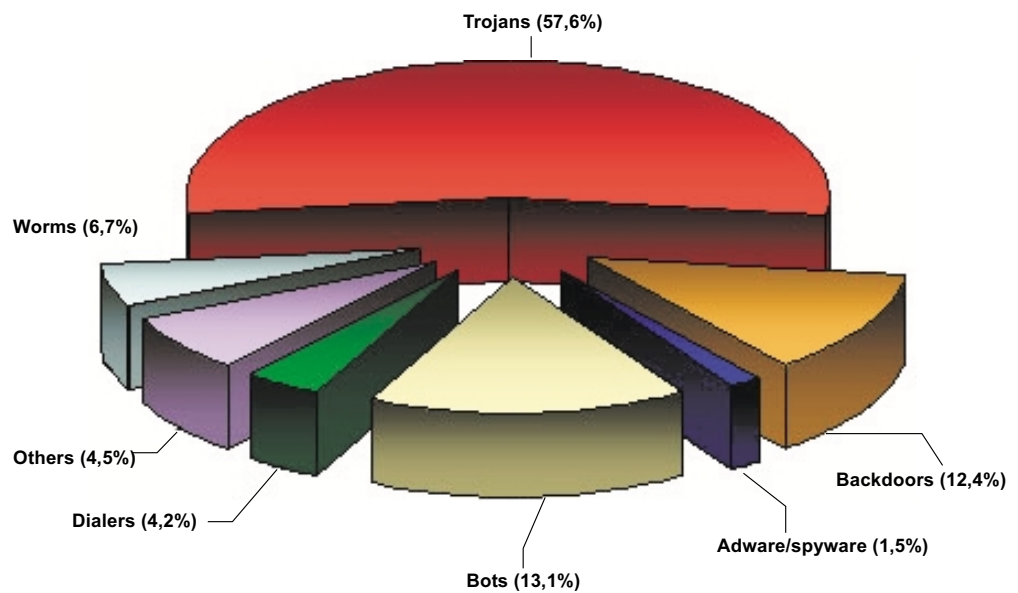


Figure 1: New Variants Detected for Each Type of Malware

As can be seen clearly at first sight, the malware category with the greatest number of new variants is the Trojan, with 57.6%. That is, more than half of all new malware that appeared on the market was of this type, and it could continue growing implacably until reaching the new expectation of 66%, which it will possibly reach in 2007.

Accordingly, when compared with Trojans, the occurrences of any other category appear to be merely incidental. The next closest category is that of bots, and data indicates that for every new bot, 4 Trojans are found.

Threats Detected by Panda ActiveScan

The following pie chart shows the distribution of detections made, during the fourth quarter of 2006, by Panda's online tool, ActiveScan.

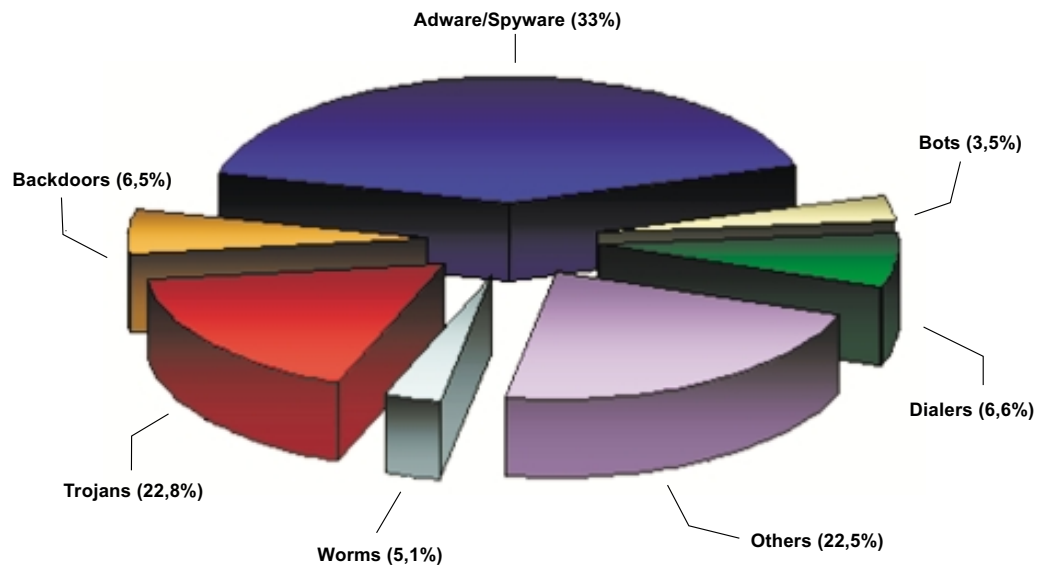


Figure 2: Types of Malware Detected by Panda ActiveScan

In the last quarter, a highly abnormal trend was perceived, which will have to be observed in the upcoming quarters in order to see whether it is confirmed or not.

The number of adware and spyware detections dropped from 40% in the third quarter to 33% in the last quarter. Even though this difference could appear to be irrelevant, it is not. The difference is accounted for on the side of the Trojans. Accordingly, even though adware and spyware continue to be the most detected types of malware, the difference that separates them from Trojans has been greatly reduced. In this last quarter, malware creators appear to have achieved their goal. Trojans are not only the category with the most new variants detected, but they also threaten to become the category generating the most infections around the world.



Malware in Trustworthy Sources

Trojans in MP3 Players

Fast food is receiving a great deal of attention at the present time. Even though the boom of the documentary, *Super Size Me*, which premiered in 2004, is now in the past, talk continues regarding the implications of the habitual consumption of fast food (also known as "junk food") on the general condition of people's health and physical appearance.

With that aside, one question that never surfaced was that of the consequences of fast food on the security of your computer, because there are consequences. The fear is no longer simply that of spilling your drink on the CPU or staining the keyboard with sauce. No, these days the fear is that of ending up infected by a Trojan.

In mid-October 2006, McDonalds Japan called back 10,000 MP3 players that users had been given in a promotion.

The promotion, founded on an agreement between Coca-Cola and McDonalds, worked in the following manner: whenever a client purchased a large soft drink at a participating McDonalds, they could then use a mobile phone to send the code printed on the soft drink in order to receive an MP3 player with 10 songs in exchange.

The promotion began at the beginning of August, and it was set to reach a maximum of 10,000 customers, but McDonalds Japan announced the MP3 players recall in October. The reason: besides coming loaded with 10 songs, these players included a version of the QQPass Trojan, which self-installed and activated upon connecting the MP3 player to the user's computer.

This Trojan is a clear example of the current malware dynamic. It is a password thief, which captures the data used to access different web services (including online banks), and then sends them by email to the creator, who can in turn use them to their advantage.

How the QQPass Trojan ended up on these MP3 players has not been sufficiently established, yet it is very likely that the system used to load the 10 songs on the players was infected and that it passed its infection on to the players.

McDonalds Japan established a phone line to provide support in the wake of this situation and to recover the infected devices. Likewise, it set up a webpage where it explained how to disinfect the systems that had been compromised.

Malware on Video iPods

Only days after the McDonalds case, Apple published a notice on its webpage that warned of a shipment of Video iPods, which had left its factory with a Windows malware. Here is the story in Apple's words:

*We recently discovered that a small number - less than 1% - of the Video iPods available for purchase since September 12, 2006, left our contract manufacturer carrying the Windows RavMonE.exe virus. This known virus only affects computers operating using Windows, and up-to-date anti-virus software, which is included with most Windows computers, should detect and remove it. So far we have seen less than 25 reports concerning this problem. The iPod nano, iPod shuffle and Mac OS X are not affected, and all Video iPods now shipping are virus free. As you can imagine, **we are upset at Windows for not being more resilient against such viruses** [bold font has been added], and even more upset with ourselves for not catching it.*

On the same page, they informed on how to eliminate RavMon from the computer, in case it had been affected upon being connected the Video iPod. Curiously, some of the recommended antivirus programs were Microsoft products (Live OneCare Safety Scanner and Live OneCare Trial). The problem emerged from one of the computers (with a Windows operating system), which formed part of the production line, that had been infected by RavMon and that ended up infecting the Video iPods with which it came in contact.

As can be seen, it is worth mentioning the similarities between this case and the McDonalds MP3 player case.

At this point, the comments are obvious. This is not a problem of whether a specific operating system is more or less affected by the malware. It is a problem of assuring that the production line, on which the Video iPods are manufactured, is free of malware and of adequately verifying this to guarantee the quality of the end product. Finding malware on the Apple production line is not Microsoft's fault; this question directly affects the Apple production processes.

Furthermore, the data offered by Apple is necessarily ambiguous. Rather than speaking of specific figures, they only speak of a percentage (1%), leaving the door open to speculation and uncertainty in regards to the number of affected users.

Of course, Microsoft did not miss this opportunity to strike back. Jonathan Poon, the supervisor in charge of ensuring that Microsoft products are sold without any malware, lashed out against Apple quality control, reminding them of their own advice, "put up-to-date antivirus protection on your own computers."



A Wikipedia Trojan Courtesy

In a very short time, Wikipedia has become a fundamental source of information for users from all around the world, and it was precisely founded with an understanding that all would contribute, creating and editing the articles that comprise it.

Since its launch, it has followed an upward trend in number of visits, and it has also gained popularity for obtaining cutting edge information in fields of all kinds, from the most "local" (try it by searching the name of your city, as small as it may be) to the most "global" level.

In January of 2007 it reached 12th place in number of visits, ahead of ebay.com, amazon.com and microsoft.com, to give some well known names.

At the beginning of November 2006, all these characteristics together (the possibility to edit the articles and its wide popularity) converted the German version of Wikipedia into the unexpected distributor of a Trojan. At least this was how it was announced at first.

Supposedly, the article, corresponding to the Blaster worm, had been edited so as to include a link to a patch that would eliminate the worm.

(Remember that Blaster, also known as Lovsan or MSBlast, was an Internet worm that appeared at the beginning of August 2003, which propagated exploiting the RPC-DCOM vulnerability. Affected computers would see a one minute countdown, after which the system would automatically restart. In order to adequately eliminate it, the first step consisted of installing the patch provided by Microsoft for that vulnerability.)

Nonetheless, the link in the article would download a variant of the Small Trojan that, after installing the true patch, would also load a new Trojan.

We speak in the conditional tense, because after confirming, it was clear that things didn't work exactly like that. What had actually occurred is that the creator of the Small Trojan had sent out a mass email with content and format similar to that of the Wikipedia pages.

In fact, the link did not point to a Wikipedia page but to another page that imitated one on Wikipedia and that was hosted on wikipedia-download.org, which was created with the intention of confusing users and making them believe they were on a page of the Wikipedia site.

Accordingly, the name and the appearance earned by Wikipedia were used to convince users to voluntarily download and run malware on their computers.



Google and the Revenge of the Kamasutra Worm

In PandaLabs first Quarterly Report of 2006, we made reference to an email worm, which Panda Software detected as Tearec.A (January 16) and which was assigned the code CME-24, but it finally became known around the world as Kamasutra.

Even though in different media, characteristics were mentioned that made it seem interesting or worthy of mention, it was nothing more than a worm that was attached to messages with erotic subject lines and which would overwrite files on the 3rd day of each month. Nothing new.

Therefore, after some days of activity, it was forgotten. At least, it was forgotten until November 7. That day, three mailings were sent to the Google Video log mail list. Then, only hours later the Google Video team admitted that some of the mailings were infected by the Tearec.A worm.

To give an idea of the scope of the situation, it is sufficient to say that the number of subscribers to the Google Video list exceeded 50,000 users at the time of the event.

It is not necessary, however, to spread an apocalyptic message. As this worm was practically one year old, any minimally up-to-date antivirus program was capable of detecting and eliminating it without any problem.

Conclusions

Hopefully, these happenings in the fourth quarter news of 2006 will serve to warn surfers. They should never lower their guard against malware.

Despite the trust inspired by a certain source or device, caution must be used at all times. In the same way files downloaded from the Internet are analyzed to verify whether they contain malware or not (because they are all analyzed, right?), it is a good idea to distrust any new device that is going to be connected to the computer or of any message received on the computer; no matter where it comes from.

The case of the Trojan in the MP3 players is nothing new. Actually, the only new angle was that this happened to be an accident. The case of an investigator that was contracted by a company to check its level of security was highly publicized this year. The investigator made a point of leaving USB keys "forgotten" (with a tracking program installed) in the company's parking lot and in other locations. The percentage of employees that connected this device to their computers, without taking any class of preliminary precaution and thus exposing their company to the theft of confidential information or to malware infection, was astonishingly high.

Do not automatically trust any device purchased, received as a gift or found. You are responsible for what you connect to your computer.

Do not automatically trust in any email message you receive, even when it comes from a source that can be identified and that is in fact trustworthy. You are responsible for the files you run on your computer; not solely responsible, but you are responsible.



Virtual Presence Attacks

Second Life: On Rings and Viscous Substances

With increasing frequency, Internet users make the leap from the real world to the virtual world. Environments like "World of Warcraft" and "Second Life", to give some examples, have become well known and attract millions of users (in October of 2006, it was estimated that the Second Life user population exceeded 1,500,000).

Nonetheless, the real and virtual worlds are not compartmentalized, one from the other. To the contrary, each one of them has repercussions on the other, and they are intimately linked. Real world money can be converted into virtual world money, and vice versa, (the equivalent of exploitation even exists; "workshops" where a person is contracted for a ridiculous price to perform mechanical actions for the purpose of earning money in the virtual world). Additionally, disputes in the virtual worlds have even developed to the point of having tragic consequences in the real world (including murder).

Considering these links between the two universes, news related to attacks against these virtual worlds becomes attractive.

However, before speaking of the attack against Second Life in November of 2006, let us discuss nanotechnology a bit. Nanotechnology is the study, design and creation of materials and functional systems by controlling material on the scale of nanometers (a nanometer is one millionth of a millimeter).

One of the dangers associated with the development of nanotechnology systems is that of "grey goo", i.e. the possibility of creating self-replicating robots that are capable of consuming all the mass in the World while they go out of control reproducing themselves.

This concept, which appears to be taken from science-fiction, appeared in full force in the virtual world of Second Life.

In this case, the subject matter is not nanorobots that are out of control, but spinning golden rings (ah, the days of Sonic), which began to appear throughout the weekend. When Second Life users tried to get their online characters to interact with the rings, these would replicate.

The situation reached such an extreme that the game experience was gravely degraded. After receiving a certain number of complaints from the users, the servers hosting the Second Life universe had to be taken off line before they could get back to normal once again; two hours later.

An object capable of replicating itself, with user interaction... Hum, this looks like a worm, exclusive to Second Life.

This could appear to be only incidental; a simple joke giving its unscrupulous creator 10 minutes of glory. Nonetheless, it is still a denial of service attack against the Second Life universe. Despite the fact that the time over which the servers were not available (and thus collapsing this virtual world) was only two hours, the possibility of overthrowing it has been demonstrated, and it could happen again.

MySpace: A New Attack to Add to the List

Once more, the introduction of news must begin with a reflection on prior events. In the PandaLabs Report from the third quarter of 2006, we made reference to a worm that was capable of propagating through MySpace profiles, which has become the social site for excellence.

On that occasion we spoke of Shockwave Flash files and how they could be used to add JavaScript code to the profile, so that all profiles visited by an infected profile would be infected as well.

Once again, we are obliged to repeat the old adage. "Those who do not learn from the past are doomed to repeat it." We can also lean on another broadly used saying, "It is not a vulnerability; it is a characteristic."

In this case, we will speak of a characteristic in the MOV format movies, which are a product of the QuickTime player by Apple. These permit the inclusion of HREF tracks, which are a special type of text tracks that are used to make QuickTime movies interactive. Web pages, which load new movies that replace the current movie, add a new viewer or load QuickTime player can be indicated using HREF tracks.

Additionally, a series of JavaScript commands can be indicated, and this is where the real danger appears; in permitting a QuickTime movie to execute commands.

The attack begins by including a QuickTime movie in a given profile. Said movie has an HREF track with JavaScript code associated so that it is able to modify the profile of any user that visits the infected profile in two different ways.

On the one hand, it includes the QuickTime movie that is creating the infection (so as to continue propagating the infection to other profiles) in the visitor's profile. On the other hand, it modifies the profile header links so that all of these point to a fraudulent website, designed to imitate the legitimate MySpace page. If the user clicks on any of the links to browse through MySpace, it will access a page that requests its username and password, which will then be sent to the author of the worm, thus compromising the profile access information.



Figure 3: MySpace User Profile Header Modified

The profile infection is particularly malicious since it is not sufficient to clean only the user's profile, but it is necessary to assure that everyone in the friends list is also clean, since the user will be infected again and again as long as this is not the case.

Up to here, this appears to be a typical worm propagation, which would be expected if still living in 2004, but we are living in 2006, dangerously immersed in the new malware dynamic so that it is necessary to hold off on that prognosis and allow this worm to bring honor in due time. Many concerns rise to the surface here; there has to be some way of taking advantage of this situation economically.



And that is exactly how it is. Besides the actions already referenced, the worm (detected by Panda Software as JS/QuickSpace.A.worm) sends spam to everyone found in the affected user's list of contacts. The messages sent contain a file that appears to be a movie, but actually it is a link to a pornographic website, which among other IT beauties, hosts adware pertaining to Zango (previously known as 180Solutions), a company that is constantly being called into question for its use of unorthodox techniques and which reached an agreement in this same fourth quarter with the Federal Trade Commission of the United States of America to pay 3 million dollars due to such dubious practices.

Accordingly, in fact this whole story actually revolves around the installation of adware on people's computers without user consent or awareness. For each installation, a certain fee is paid. By infecting more profiles, more installations will be made and with more installations more earnings are generated.

At the time of stopping the worm propagation, the problem resides in the fact that it was not a QuickTime movie vulnerability being exploited. Instead it was a characteristic, so treating the problem was not a matter of patching the vulnerability; it was a matter of Apple eliminating the functionality.

According to MySpace, the number of users affected by this worm's attack could have reached as many as 100,000.

Three days after the attack, the only solution that Apple could give was a patch that deactivated said QuickTime characteristic, using Internet Explorer. It was MySpace's responsibility to distribute the patch. At the same time, this provisional solution left the users of other browsers defenseless. Even though Internet Explorer dominates the markets, other browsers, such as Firefox and Opera, are widely distributed to the users (for example, in December of 2006, Firefox alone accounted for more than 30% of the total).

Additionally, what happens to the users that DO NOT have a MySpace profile? Can they request the patch from MySpace? Will they be exposed to more unscrupulous treatment to exploit that same characteristic?

Conclusions

One of the immediate readings is that the MySpace security leaves much to be desired. The problem with worms capable of infecting and modifying profiles is that it occurs time after time, and it appears that the company only focuses on reacting and that it does not learn from the errors of the past. Nonetheless, we cannot stick with a reading that, although true, is quite simplistic.

With increasing frequency, Internet users decide to make their presence in the virtual world. Online games and social sites are only some of the territories that are making ground in the number of interested persons. For fun or as an alternative to the real world, people from all over the world are being attracted.

Out there where there are herds of possible prey, the predators are lurking, and if it is possible to relieve that prey of their weighty wallets, the predators will try to find every way possible to do so.

User protection cannot be solely based on the technical means deployed by a site in question. As commented previously, the user is just another link in the chain of security and is the protagonist and the one responsible for his or her own security. Even though there are driving regulations, signals that must be used, and police to supervise compliance with the rules of the road, "would you cross the street without taking some minimum precautions?"



Alarm over the Skype Worm

Skype: The Popularity of IP Telephone

IP telephone, also known as Voice over IP or VoIP, is a technology that permits the carrying out of audible conversations over a network based on IP protocol (over the Internet for example).

Notwithstanding the great advantages offered by this technology, it has been delayed some time in reaching a point of maturity due to the difficulty in overcoming its main problem: guaranteeing the quality of service.

There are various points of focus when using an IP telephone. One of these has to do with the installation of a software client on the computer, which is then charged with managing calls over the network. To date, the best known and most used at the present time is Skype.

Its interface is very similar to that of an instant messaging software, and in fact, it permits conversations via instant messages with other users in addition to conversations via telephone calls.

Skype Worm: First Contact

On December 18, Websense Security Labs published a warning in its "Threat blog" in which it confirmed the receipt of various incidents of a new worm, which was utilizing Skype to propagate itself.

Preliminary data made available explained it as follows: Skype users receive a message via Skype Chat, inviting them to voluntarily download and run a file called sp.exe. Then, the file will install and run a password stealer type Trojan. The sp.exe file is also capable of using the Skype API to send itself to other users.

Although the number of incidents remains undetermined, they were geographically located in Asia – Pacific, specifically in Korea.

With more than 7 million users throughout the world, the possibility of one worm being capable of using Skype to automatically propagate and distribute a Trojan was bloodcurdling, and the story was sufficiently juicy for the different websites on the Internet to begin to echo the news in record time, basing this on little more than the Websense message.



The Smoke Clears

The following day, after studying this more in-depth and gaining clarity, Websense published a new article to better define the scope of the threat and its typology.

In fact, what had been prematurely cataloged as a worm (with capacity to self propagate) was actually a Trojan (manually distributed or at least not self-distributed).

Just as had been concluded after the Skype security team collaborated with Websense, a software vulnerability was not being exploited to allow the malicious file to automatically distribute. The Trojan used the Skype API just as any legitimate program could, and required user interaction to download and run on the computer.

Conclusions

While the primary objective of the malware was to achieve economic gain, getting the attention of the security companies and that of the users by creating a situation of alert did not turn out to be an advantageous move.

An alert implies getting the attention of the press and raising user awareness (even if only temporary) causing them to install new solutions, update existing ones or adopt new means of protection. From this point of view, it is highly improbable that a situation of heightened alert, due to a similar malware will be relived (unless this has to do with some way of redirecting attention, a fake alert that focuses all efforts in a different direction just as magicians use the technique known as "misdirection").

Nonetheless, one of the labors of the security companies is precisely that of operating as observatories watching over the situation of malware on the worldwide level. Although warnings of this type can sometimes seem something more like the story of "The Boy That Cried Wolf", they are useful when keeping users informed. Precise and up-to-date information is one more weapon in the arsenal of measures that can be deployed against malware.

It is also true that this work should be done with the greatest objectivity possible in order to avoid creating artificial alerts, which improve sales, but only make a currently confusing situation even more so.

A warning sign on an ending note: although email messages and web pages that use browser vulnerabilities are the most used methods, they are not the only ones out there. If cybercrooks are distinguished by anything, it would be the new distribution vectors they use, which can be silently disseminated, without raising any suspicions, resulting as novel and inconspicuous.



A Christmas Story

Social Engineering

Before beginning to speak on how the 2006 Christmas season went in regards to malware, we will provide a small introduction so as to center in appropriately on some concepts.

To understand why Christmas is a particularly cherished time for malware creators, we must have a basic understanding of social engineering and the mechanisms it uses.

Social engineering is a collection of techniques used with the objective of manipulating legitimate users into performing certain actions or providing confidential information.

It is a technique that is highly used above all in malware distribution. Most email worms and Trojans trust in social engineering techniques, which are more or less elaborated to be run voluntarily by the user.

Although they were some time ago, perhaps you will remember the case of the Kournikova or ILoveYou worms. Both based their success on the careful choice of social engineering. Who would deprive themselves from opening a file that says it contains photos of Anna Kournikova or has a love letter?

This is precisely the heart of social engineering applied to the distribution of malware, selecting themes that are most likely to get a user to show their willingness to take a risk and run a certain file that was not previously requested.

The most used themes (not necessarily in this order) are the following: sex, famous people, current news (including the Soccer World Cup), kinky themes, errors in sending an email, etc. "Seasonal" themes, used to their maximum extent on Valentine's Day, Halloween, Christmas and New Years Day, deserve a special mention.

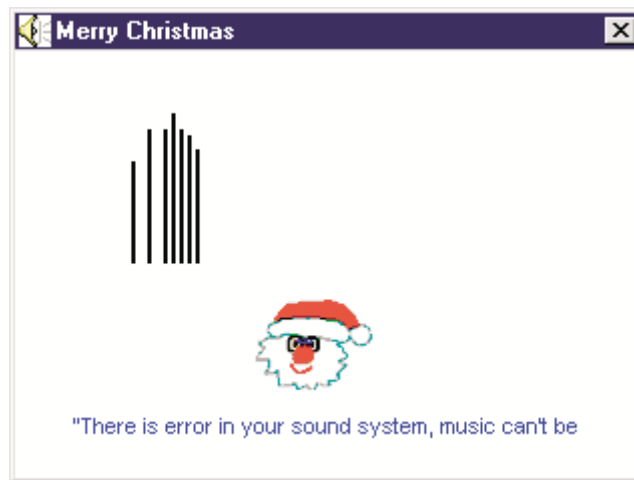
Christmas is a season in which it is very common for users to send and/or receive messages, photographs, videos, PowerPoint presentations and Flash files for all types of seasonal reasons. Given that this is so common, it is easy to lower one's guard and not analyze everything that comes into the computer.

The Spirit of Christmas Past

With a clear understanding of social engineering and how it applies to Christmas, let's take a look at the examples of this type of malware from previous years. As we are about to prove, this is nothing new.

Music (December 2002)

An email worm with no destructive effects comes out, which plays a melody and shows messages on the screen:




Maldal.C (December 2003)

An email worm that blocks the keyboard. This is propagated via a Flash animation and appears as follows:



Zafi.D (december 2004)

As the climax of the “year of the worm”, Zafi.D wished people a Merry Christmas in various languages (depending on the extension of the domain to which it was sent). It was capable of being sent in up to 14 different languages and caused an orange alert.

Subject: Fw: Merry Christmas!
Attach:  link.postcard.christmas.php6827.zip (11,9 KB)

* Happy.... Hollydays! *

:) Pamela M.

<http://link.postcard.christmas.php6827> - Picture Size: 11 KB, Mail: +OK

Atak Family (December 2004)

This was a family of worms that lived its moment of glory at the end of 2004, and were propagated by email in messages that included images and typical texts of the time.

Happy New year and wish you good luck on next year!

Mery Chrismas & Happy New Year! 2005 will be the beginning!

Merry X.A (December 2005)

This was a password stealer type Trojan, which also downloaded other malware onto the computer. It would show up by way of email in messages that included the following images and movies.





Besides seeing different examples of malware focusing on the Christmas season, we can also make a second reading on that which we find in abundance in this annual report. In previous years, malware used in the Christmas theme to hook users into running it did not have destructive effects per se. However, in 2005, we have referenced a password stealer type Trojan, which used this technique.

The Spirit of Christmas Present

Accordingly, the type of malware that uses the Christmas season as an excuse to be distributed comes as no surprise, and there is certainly no shortage of examples.

1. A PowerPoint, commonly referred to as Christmas+Blessing+4.ppt. The content of said presentation has been modified so that it includes an exploit for a Microsoft PowerPoint vulnerability, solved by the MS06-012 bulletin (March 2006). If the malicious presentation is opened on a computer, that has not been patched, it will install two Trojans.
2. An executable file called Christmas.exe, which shows a Christmas image while in the background it installs a copy of IRCBot, converting the computer into part of a botnet.
3. A puzzle with Christmas images, whose file was commonly called Christmas_Puzzle.exe. Actually, this was a Trojan that would capture keystrokes. It used a rootkit to hide on the computer and make removal difficult.

In summary: Trojans that install themselves by taking advantage of vulnerabilities, bots and Trojans that use rootkit techniques were all used under the innocent guise of a Christmas message.



Conclusions

Just as the spirit of Christmas yet to come, the outlook for the upcoming Christmas seasons is gloomy.

All signs point to the fact that malware will continue along the lines of its current dynamic, seeking economic gain at the cost of the users, whether directly or indirectly.

Regardless of the fact that the same thing happens on the same dates, it is clear that this model functions because it continues to perpetuate. Crimeware will continue to repeat the themes that result in a greater percentage of fooled users.

In the same way that Ebenezer Scrooge was capable of learning from the complete vision of his past, present and hypothetical future, and changing his conduct in order to redeem himself, we users must set the goal of changing our conduct in order to minimize our attack surface for being bombarded by outbursts of malware.

One of the first steps is to immunize against the effects of social engineering. The important questions are: Did you request this file? Are you absolutely sure that this is really what it claims to be? Can you find references to some similar case of malware in a search engine?

If rather than running the attached files that arrive by email (blindly trusting in the sender, whether known or unknown), you take the time necessary to save them to the hard disk and analyze them with an up-to-date antivirus program, which includes proactive technologies (heuristics, behavior analysis, etc.), a multitude of infections would be avoided.

2006 in Perspective

Distribution of New Threats Detected throughout the Year

The following pie chart shows the distribution of new variations of malware types, detected by PandaLabs during the whole 2006 year:

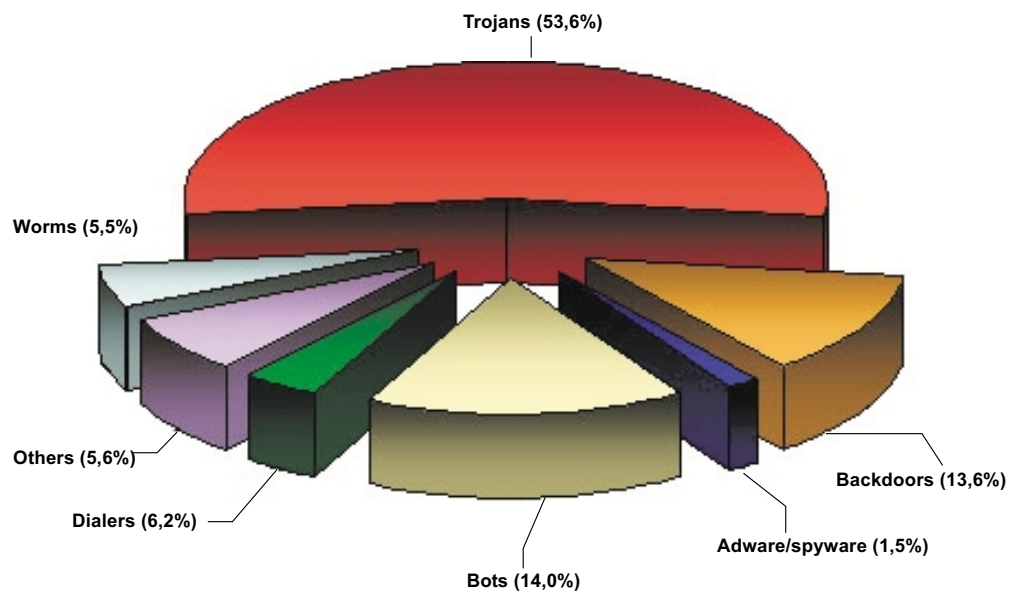


Figure 4: New Variants Detected for Each Type of Malware in 2006

This pie chart, which summarizes the whole year, offers no surprises, and it does no more than confirm the panorama that has been witnessed over each one of the quarters. The Trojan is the malware category for which the most new versions appear. Along these lines, more than half of the new malware that appeared in 2006, pertained to this type.

Accordingly, it can be used for clarification to verify the tendency of the appearance of new malware categories over the four quarters of 2006:

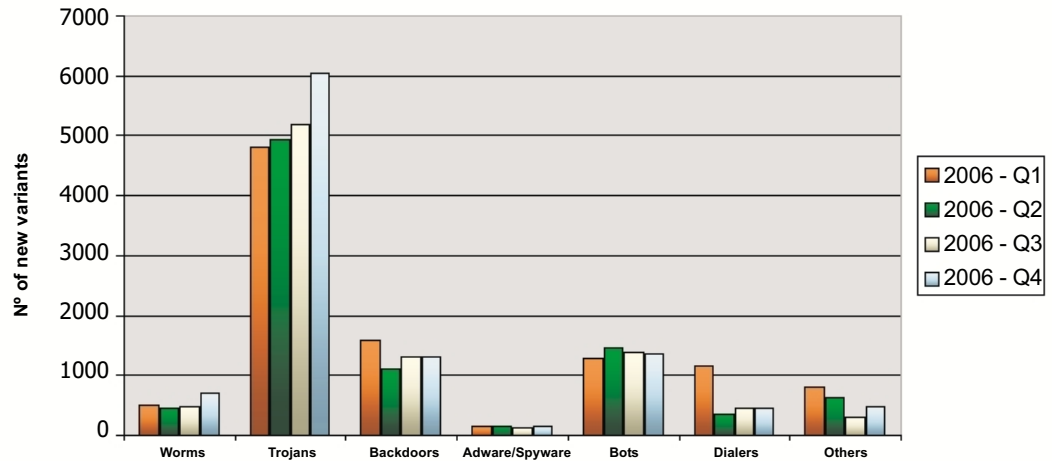


Figure 5: Comparison of New Variants that Appeared over the Four Quarters of 2006

Firstly, and due to their unrivalled prominence, we must speak of the Trojans. This is not only the category that can presume to have more new variants, but it also fulfils a rare condition. It is the only category that has not suffered from ups and downs.

The number of new Trojan variants has been gradually increasing always with an upward trend. Remember, in order to leave the data clear, that the figures grew from 47% (first quarter) to 57.6% (fourth quarter), i.e. an increase of 10% in only one year. A figure that is certainly neither trivial nor incidental.

Backdoors and bots are battling for second place, but these remain well behind the Trojans up front. Both categories share the commonality of being able to permit the affected computer to be remotely accessed and controlled. While backdoors appear to show a slightly downward trend, bots are gradually increasing.

As for the categories that are clearly declining, dialers for example (in the previous quarterly reports, we pointed out their progressive disappearance from the market based on wide scale access to broadband Internet), and the "others" category (corresponding to the rest of the categories not considered: viruses, hacking tools, etc.), adware and spyware continue to be stable although they have low levels in the number of new variants.

Worms are worthy of special mention. These were the clear protagonists of the years 2003 and 2004 although they are far from their glory days, they have not relinquished to completely disappear from the market, and even though the figures are quite modest, they continued to be present and growing in the last quarter.

Threats Detected by Panda ActiveScan during 2006

The following pie chart shows the distribution of detections made, over the whole year of 2006, by Panda's online tool, ActiveScan.

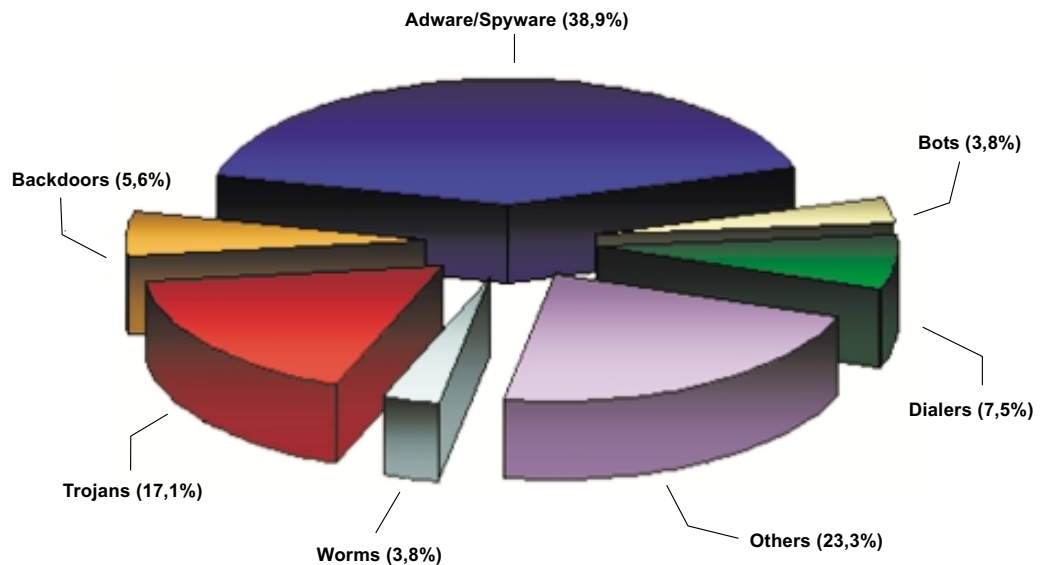


Figure 6: Types of Malware Detected by Panda ActiveScan in 2006

Once again, we find no great surprises here. As already happened in most quarters of 2006, adware and spyware continue to hold their ground in the computers of users around the world. Of every 100 infected computers, nearly 40 have some example of adware or spyware internally.

The miscellaneous category that groups virus, hacking tools and other similar types, is to be found some distance behind. Trojans follow, being found on "only" 1 in every 6 infected computers.

The true surprise, as we demonstrated in the fourth quarter 2006 review, is seen when we compare the infections produced over the whole year, grouped by quarters:

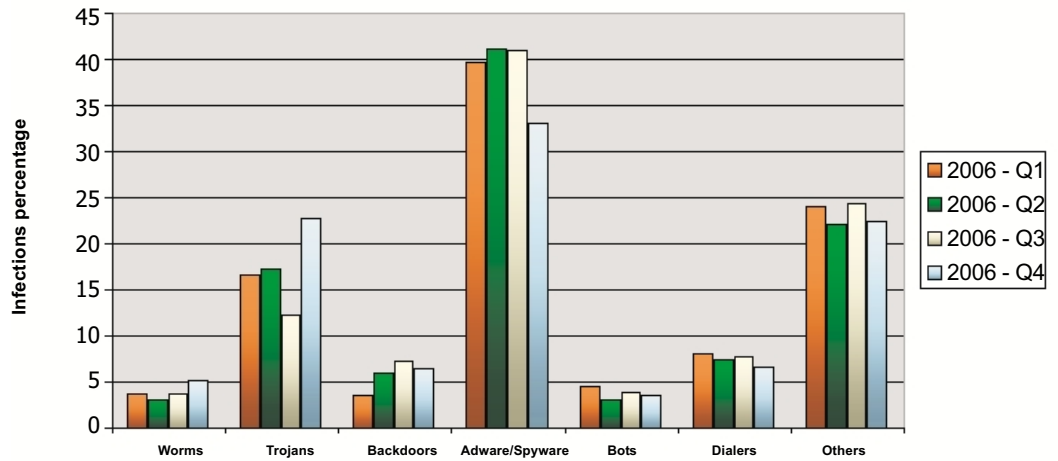


Figure 7: Types of Malware Detected by Panda ActiveScan

During the first three quarters, we attended to the maintenance of the status quo: the existence of a high number of adware and spyware infections while the rest of the categories oscillate in a stable manner around a mean.

Nonetheless, the fourth quarter of 2006 could have marked an inflection point. Infections by Trojans shot up. We must wait to see if this tendency holds in the upcoming months.



Evolution of Malware Categories in 2006

Worms

Worms are used not as an end in themselves but as a means to reach other objectives. One of the clearest examples is the Spamta family. This is a malware family with the objective of converting the user's computer into a computer used to send Spam.

The case of the Tearec.A is no more than incidental. It was only an exaggeration by the press, which continues to wait for the alerts of old.

As for the rest, a small increase was observed in this category during the last quarter of the year; this was probably due to worms using the Christmas theme.

Trojans

Trojans are the center of the current malware model.

In days of old, the perception could be that reach was very limited since they could not self-propagate.

Nonetheless, that distribution model is an advantage today. It is silent and directed. Non-discriminated propagation is not used. It can be sent to chosen parties or to the whole world if preferred (the day will come when all email addresses in the world, which have a certain age, appear in spammer's databases and receive malware).

It can be said that a Trojan is a limited bot. Rather than having been programmed to receive a set of orders executed on demand, it has been programmed for a limited set of functions, which are executed independently.

The level of perfection and the specialization of this category is obvious when its level of increase is observed one quarter after another.

Backdoors

This category holds stable, which may be due to the fact that the essential functionality that determines it as a category is beginning to be integrated into more complex products such as Trojans that now incorporate backdoor functionalities.



Adware/Spyware

Commonly, adware and spyware attain very high levels of infection due to the way they are distributed. They are included within other supposedly useful software, which the user installs without carefully reading its End User License Agreement. They are installed from malicious web pages that exploit web browser vulnerabilities. They are passed off as programs of all kinds, from browsers to codecs for movies. They are installed from botnets (a multitude of compromised computers, administrated together as a network). They are installed by downloader type Trojans.

Additionally, the degree of user sensitivity for this category is not sufficiently high. Confronted by its effects, many users do not esteem it highly enough given that they do not see the problem with privacy, represented by showing the announcements or watching their browsing habits.

Bots

Another evolution in the backdoors category are the bots, which permit control to be gained over an ever increasing number of computers. The greatest weakness of these networks is that they are centrally controlled.

In the past, these networks were typically controlled from a single IP, which made it possible to disconnect the network once the server was located. Currently, DNS services are used, which makes it possible to reconnect a server and regain control over the network.

To make them more persistent, it has been observed that they are beginning to modify the control protocols, passing from IRC to modified versions of IRC. In accordance with the firewall configuration, it avoids accessing non-standard ports and it will produce a migration to protocols such as http as well as the use of P2P networks, which makes it very difficult to stop the networks as at this moment there is no longer a central control node.

Dialers

As it is currently understood, the future of dialers is linked with telephone access to the Internet. As this method of access is being abandoned in favor of other technologies such as ADSL, cable, WiFi, etc., dialers will disappear from the market, at least in the first world countries.

It remains to be seen how Internet access will be obtained in developing countries after new initiatives such as that of the 100 dollar computer. If they adopt telephone access as their method of choice, we could witness a new surge in this category. Nonetheless, this does not seem probable since deployment in these countries is very expensive as they do not have the prior infrastructure. What's more, there are several companies working on employing WiFi technologies, which could be the solution.



What Can We Expect from 2007?

Here we will attempt to look into the future, and provide a summarized forecast of the evolution expected in the different categories for the upcoming year.

The downward trend in worms and viruses observed throughout 2006 will be maintained. Malware creators see no benefit in mass propagation, which only cause losses of millions to companies and some press owners. The end goal is now financial gain.

Adware is evolving into an industry in which pay per installation businesses are flourishing. New techniques such as false codes, permit installations to be made daily in thousands of computers, which are then infected by adware. Additionally, the installations become more sophisticated in order to make their detection more difficult, to hide them better, for coding, etc.

Spyware resembles other categories, incorporating the capacity of information theft as an additional functionality. An example includes bank Trojans, which specialize in electronic bank information theft, Trojans that rob online game passwords, etc. This fusion will make the barriers that separate different families (worms, Trojans, etc.) as we currently know them, become more difficult to establish in 2007.

The ever increasing appearance of more supposed antispyware, which is actually no such thing, can have negative consequences on the industry, which are damaging to its credibility.

We close 2006 reading reports that speak of how 90% of all email traffic is spam. Is there a solution? Yes, but users must understand that there is no perfect technological solution and that they will have to collaborate. As long as product or service purchases announced by spam continue to exist, even though this is a small percentage, the spammers' business model will continue to function, and they will have no reason to change this activity. Along those lines, the levels of spam reached in 2006 will be maintained in 2007.

Exploit-based attacks will increase. It appears that the black market for vulnerabilities is clearly at a peak, and we are continually seeing news about prices of more than 10,000 dollars being awarded for an unpublished vulnerability. It is true that the same industry has taken some initiative to purchase these vulnerabilities, but the prices they pay, 5,000 dollars versus that of 15,000 dollars paid on the black market, do not provide great incentive for collaborators.

In the case of virtual worlds, we have learned of the first attacks. If an economic loss was not inflicted in the case of the Second Life worm, economic losses were a reality of the WoW case (World of Warcraft). In the latter case, users saw how they were robbed of their virtual goods to turn around and exchange them in online auctions for real money. An online auction company recently stopped auctioning objects that pertained to one of these virtual worlds. In this way, it is probably easier to avoid being accused of favoring the commerce of stolen "merchandise".

As the link between the virtual and the real world becomes stronger, and profits can be extracted to be exploited and abused in this type of environment, we will see more sophisticated attacks on the rise.



During this year, we have seen apparently inoffensive devices such as MP3 players, PDAs, etc. appear contaminated by malware during the manufacturing process; these could have infected many users. Device quality control should guarantee that it is 100% free of malware since these portable devices are heavily used by their owners, who share them between computers at home, work, cyber cafes, with friends, etc. By this, we are reminded not to forget that problems do not only come from files downloaded from the Internet, but there are also other ways on being infected.

It is also important to remember that some of the most damaging attacks, from the financial point of view, are phishing attacks, which do not require complex techniques but rather lean on the use of social engineering. In 2007, an upward trend is expected since the new techniques used, with more highly directed attacks, increase the ratio of success.

The distribution of malware via email, disguised as mail containing current news events, disasters, politics, etc., confirms that users continue to trust in emails coming from unknown sources.

Maybe we should consider that the weakest link in the security chain is currently the user, and it will be necessary to insist on their education as a means, not to diminish, but at least to ease the effects of this whole epidemic.

Laptops and planners are stolen; hard disks and travel drives are recycled. There is a lot of uncontrolled information that, in the wrong hands, permits making directed attacks.

To wrap up, we close the year with the expectation of the appearance of Windows Vista with new security functionalities incorporated; the weight of great expectations burdens its shoulders. We hope these expectations will be fulfilled, and that we will have a world with less malware.

New Threats

Evolution has been observed as malware creators acquire experience and resources, exchange code, sell malware creation kits, rent bot networks to carry out spam attacks, etc. All these attacks continually become more sophisticated.

The upward trend in the number of each malware family's different variants will be maintained since the ever increasing specialization of the different types of malware results in a shorter "useful" life for each variant. Automatic malware creation tools facilitate the distribution of multiple variants within a single day. Therefore, the numbers of new malware registered in 2006 will hold their ground and may even increase.

The more and more generalized use of code packers, a simple way of making code analysis more difficult, marks an important challenge to the industry's antim malware laboratories.

Finally, we must not forget that users will continue to play a primary role in the security chain. We offer the following scenario as an example:

A user tries to see the content of a page, and said page requests permission to install a false codec. Even though the user finally decides not to install it, an exploit used on the page installs a rootkit, which hides the installation of a Trojan.



This Trojan is not only charged with downloading a series of control applications to the computer, which turn it into a zombie for sending spam, but it also periodically updates itself, installing keyloggers, which focus on stealing certain banking data. Once personal data is obtained, a directed phishing attack turns the user into a perfect target.

It has taken much time to raise public awareness of the dangers supposed by viruses and worms. Nonetheless, as threats become more complex and antivirus companies evolve into antimalware companies, user education lags a bit behind.

The technological complexity exhibited by some variants, combined in the same cocktail of rootkit, Trojan, spyware and backdoor functionalities is not reflected on the concepts handled by the average user.

All this should make us reflect on the scale of this problem. Only by embracing a global vision, which includes not only the technological solutions but also the users, can we progress to resolve the same.



About PandaLabs

PandaLabs is an antimalware laboratory of Panda Software, and it represents the neurological heart of the company in terms of handling the referenced malware:

- In real time and without interruptions, **PandaLabs** draws up the countermeasures necessary to protect the Panda Software customers from all types of malicious code around the world.
- **PandaLabs** carries out detailed analyses on all types of malware with the objective of improving the protection offered to Panda Software customers and to inform the public at large.
- Along the same lines, **PandaLab's** continuous surveillance closely follows the different trends and occurrences in the field of malware and security. Its objective is to provide warnings and alerts as to the imminent dangers and threats as well as forecasting those of the future.