



Quarterly Report
PandaLabs

(July – September 2006)





Contents

Introduction	5
A Day-by-Day Report of the Quarter	6
July	6
August	7
September	8
Quarterly Figures	9
Distribution of New Threats Detected	9
Threats Detected by Panda ActiveScan	11
July – The Month of Browser Bugs	13
Fuzzing Tools, Errors and Vulnerabilities	13
Results Obtained and How to Interpret Them	13
Informing Users about Vulnerabilities	15
Reactions to the Month of Browser Bugs	15
Repercussions	16
Conclusions	16
Vulnerabilities in Microsoft PowerPoint	17
Attack of the Malicious Presentation	17
Details of the Vulnerability	18
A Certain Feeling of Déjà Vu	18
Don't Go Yet, There's More	19
Conclusions	19
End of Support Phase for Windows Millennium and Windows 98	20
An Unpromising Start for Windows 98	20
Windows Me - Criticized and Short-lived	20
Implications of the End of the Extended Support Phase	21
Conclusions	22
MySpace in the Line of Fire	23
Those Who Cannot Remember the Past are Condemned to Repeat It	23
A MySpace Banner Distributes Malware amongst Users	24
Conclusions	25



The strange case of the MS06-042 patch	26
Accumulation of vulnerabilities.....	26
Something stinks with the MS06-042 patch.....	26
A solution that introduced new critical vulnerabilities.....	27
And again and again!.....	27
Third time lucky.....	28
Conclusions.....	28
After the patches, then comes the malware	29
The MS06-040 Bulletin.....	29
First public sighting: Oscarbot.KD.....	30
Onwards and Upwards.....	30
A secondary shock: MS06-047.....	31
Conclusions.....	31
The Consumer Reports 5,500	33
A brief introduction to Consumer Reports.....	33
Analyzing discord.....	33
It is not necessary and it is not useful.....	34
Not a one-sided battle.....	34
Conclusions.....	35
Google and malware	36
Google solves a vulnerability in its RSS reader.....	36
Google indexes executable files.....	36
A Trojan disguised as a Google toolbar.....	38
Google to warn of malicious sites.....	39
Conclusions.....	40
Orange Alert	41
Phishing/BarcPhish.HTML.....	41
Great number of active malware.....	43
Conclusions.....	45



Other news in short	46
America On Line publishes its users' searches	46
25th anniversary of the PC	46
CarderPlanet: malware professionals	46
Spamta worms: first contact	47
Vulnerability in Vector Markup Language (VML)	47
About PandaLabs	48



Introduction

If we had to choose a word to summarize the Quarterly Report you are about to read, the choice would be obvious: vulnerabilities.

All sorts of vulnerabilities: in web browsers, in office tools, in picture files. Vulnerabilities whose patches have to be re-released several times, and vulnerabilities whose patches are the target of reverse-engineering in order to create an exploit. Zero-day vulnerabilities, and vulnerabilities which are months old but which have still not been patched by some users.

This PandaLabs report, which summarizes the third quarter of 2006, helps to visualize the presence, discovery and exploitation of vulnerabilities in the context of today's malware dynamic, which is centered on fraudulent financial gain.

The report is also full of numbers: 25 years of personal computers, 5,500 new viruses created by Consumer Reports, 658,000 America On Line users, 1,000,000 MySpace users affected by spyware, 70 million Windows 98 and Millennium Users.

Throughout the report, we have tried to list events in chronological order. In some cases, however, we have grouped events together because of similarities that they share, with the aim of creating a clearer picture of the issue as a whole.



A Day-by-Day Report of the Quarter

July

- Day 1.** The Month of Browser Bugs begins.
- Day 2.** Panda Software detects Peerbot.B, a worm which obtains information from SQL Server and MySQL databases.
- Day 3.** A user files a lawsuit against Microsoft over its Windows Genuine Advantage program (which contacts Microsoft servers daily), alleging that the application is a form of spyware. A researcher compromises the Microsoft fingerprint reader. OpenOffice publishes a security update for 3 serious vulnerabilities.
- Day 4.** In October, Hewlett-Packard will commercially launch a tool which uses techniques similar to those used by Internet worms to identify vulnerable computers which need security patches within a network. Five youths between 19 and 24 years of age are accused of illegally accessing a LexisNexis group database.
- Day 6.** Panda Software detects Gatt.A, a virus which infects IDA disassembler files. Google repairs a security fault in its RSS reader. French Security Incident Response Team (FrSIRT) discovers a new vulnerability in Excel.
- Day 7.** Experts warn of potential attacks based on techniques similar to those used in steganography. Experts warn that it is possible to create videos using screenshots from next generation H-D DVD and Blu-Ray DVD recorders. A telephone phishing attack is carried out against PayPal users. Google is capable of carrying out binary searches in files.
- Day 8.** Remote code execution can be carried out using a malicious Word document which exploits the mso.dll library.
- Day 10.** Panda Software detects Semsy.B, which steals Orkut passwords.
- Day 11.** Microsoft publishes 7 security bulletins (MS06-033 to MS06-039). One of these deals with the Excel vulnerabilities mentioned in the last Quarterly Report. The Microsoft Windows 98 and Windows Millennium technical support phase comes to an end. Adobe publishes a security patch for Acrobat Reader. eBay's Picture Manager could be used to compromise computers. WebAttacker becomes the most popular exploit, ahead of WMF.
- Day 12.** At least 2 Excel vulnerabilities have not been solved using the previous July's patches. A Gmail phishing message offers a 500 dollar prize to lure its victims. Researchers at Cornell University crack the system codes of the European satellite navigation project (Galileo).
- Day 13.** A zero-day vulnerability in Microsoft PowerPoint is discovered.
- Day 14.** First sightings of a Trojan which exploits a PowerPoint vulnerability. A Chinese company cracks the Skype protocol. A website uses the altercation between Zidane and Materazzi as a ruse for spreading a Trojan.
- Day 15.** Panda Software detects PPDropper.A, which exploits the zero-day vulnerability in PowerPoint.
- Day 16.** A new attack against MySpace, using a Flash worm. A banner on MySpace exploits the WMF vulnerability in order to install spyware on users' computers.
- Day 17.** Microsoft publishes a security warning regarding the PowerPoint vulnerability.
- Day 19.** Microsoft acquires Winternals Software, and the renowned professional Mark Russinovich joins the Microsoft team.



Microsoft plans to develop a program similar to Windows General Advantage for its Office package.

A widespread Trojan poses as the Google toolbar and turns computers into zombies.

Day 20. Oracle publishes its quarterly security updates.

Day 21. Graham Ingram, director of AusCERT, recommends avoiding top-selling antivirus solutions.

Day 23. Panda Software detects Snifsteal.A, a modified version of a Firefox extension.

Day 24. Panda Software detects ASPLux.A, which infects ASPX files.

Day 25. Panda Software detects Dengis.A, a new virus affecting Matlab source files.

At the HOPE (Hackers on Planet Earth) conference, demonstrations are given showing how to clone an RFID chip in order to pretend to be its legitimate owner.

Day 26. Microsoft will provide automatic Internet Explorer 7 updates.

Mozilla publishes various security updates for its products.

Day 27. A federal agent in Florida has his laptop stolen, putting the data of 133,000 Florida residents at risk.

Day 28. The United State Navy admits that a computer containing the personal data of 31,000 soldiers has been lost.

Day 31. The Month of Browser Bugs comes to an end.

A Firefox web browser exploit is published.

August

Day 1. Apple publishes patches for various Mac OS X vulnerabilities.

Day 2. A vulnerability which allows denial of service attacks in the RRAS service is discovered. Reports state that it is possible to compromise a Mac computer via its WiFi drivers in less than 60 seconds.

Day 4. The fourteenth DefCon conference begins in Las Vegas.

DefCon talk: JavaScript attacks.

DefCon presentation: CarderPlanet, malware professionals.

Day 5. Throughout the weekend, America On Line publishes details of searches carried out by 658,000 of its users.

Day 6. The 14th DefCon conference comes to an end.

Day 7. Google will warn users about the potential risks present in some sites appearing in search results.

Day 8. Microsoft publishes 12 security bulletins (MS06-040 to MS06-051). One of these deals with the PowerPoint vulnerability.

A Windows CE vulnerability will allow automatic propagation of a cell phone worm.

Day 12. 25th anniversary of the commercial launch of the first PC.

Day 13. The Oscarbot.KD worm, which takes advantage of the MS06-040 vulnerability, is detected for the first time.

Day 15. The first variant of the Spamta worm family is detected.

News that Consumer Reports magazine creates 5,500 new viruses to carry out a comparative analysis of antivirus programs begins to spread.

Day 17. Malware which exploits the vulnerability resolved using patch MS06-047 appears.

Day 19. The application of security patch MS06-042 may cause problems with Internet Explorer.

Day 21. Microsoft plans to launch the corrected MS06-042 patch for IE SP1 on August 22.

Day 22. The publication of patch MS06-042 is postponed when it is discovered that the patch could cause a new vulnerability.

The CTO of America On Line resigns after the scandal of the disclosed user searches.



- Day 25.** Microsoft re-releases the MS06-042 patch and removes eEye from the list of credits.
- Day 26.** Councils in England install surveillance cameras in garbage bins.
- Day 28.** A bot owner is sentenced to 37 months in prison after his bots affected several hospitals.
An antivirus company warns about phishing attacks via SMS.
A password-stealing Trojan poses as a Microsoft patch in order to convince users to execute it.
- Day 29.** The SANS institute warns of a sharp increase in registration of domain names related to hurricane Ernest which could be used to carry out fraud.
Sun releases a Java Runtime Environment patch to solve a vulnerability which means that older versions (which have not been uninstalled) can be used.
.es domains are inaccessible for 2 hours.
- Day 30.** Credit card thieves hack the AT&T online store.
- Day 31.** Malware which gives false Internet search results is detected.
A vulnerability is detected in the Playstation Portable console.

September

- Day 1.** A man who provoked security faults in companies and then solved them for a “reasonable” price (up to 84,000 euros) is arrested.
- Day 4.** 3 hackers are arrested for attacking the web pages of various companies (COPE, Telemadrid, Menéame).
- Day 5.** A new zero-day vulnerability is detected in Microsoft Word: a malicious Word document uses the vulnerability to download malware to the computer.
Spam messages using subliminal advertising techniques are detected.
- Day 6.** The US-hosted Samsung Electronics web page is found to be hosting malware.
- Day 7.** Microsoft releases a patch for its DRM (Digital Rights Management) system 3 days after discovering that the system has been compromised.
- Day 12.** The 2 men arrested for creating the Zotob.D worm are sentenced to between one and two years in prison.
Panda Software declares a state of Amber Alert due to a huge increase in phishing messages targeting Barclays Bank: Phishing/BarcPhish.HTML.
Microsoft publishes 3 security bulletins in September (MS06-052 to MS06-054).
- Day 17.** Panda Software detects Sohanat.A, an instant messaging worm which takes advantage of a flaw in the MSN Messenger PIF files filter (the filter was case-sensitive).
- Day 19.** Zero-day vulnerability in Internet Explorer: Vector Markup Language (VML).
- Day 21.** Panda Software declares a state of Amber Alert to reflect the current malware situation and to highlight the large amount of malware in circulation.
- Day 25.** Spamta.CY poses as a security patch to avoid being affected by some vulnerabilities.
- Day 26.** Microsoft publishes the solution to the VML vulnerability (MS06-055). This publication does not follow Microsoft's usual publication routine.
A new zero-day vulnerability is detected in Microsoft PowerPoint.
- Day 27.** Microsoft begins legal action against a hacker who circumvented its copy protection system, supposedly by accessing the company's proprietary source code.
- Day 29.** The WebViewFolderIcon error described by expert HD Moore during his Month of Browser Bugs project is not a denial of service attack but arbitrary code execution.

Quarterly Figures

Distribution of New Threats Detected

The diagram below shows the distribution of new malware variants detected by *PandaLabs* in the third quarter of 2006.

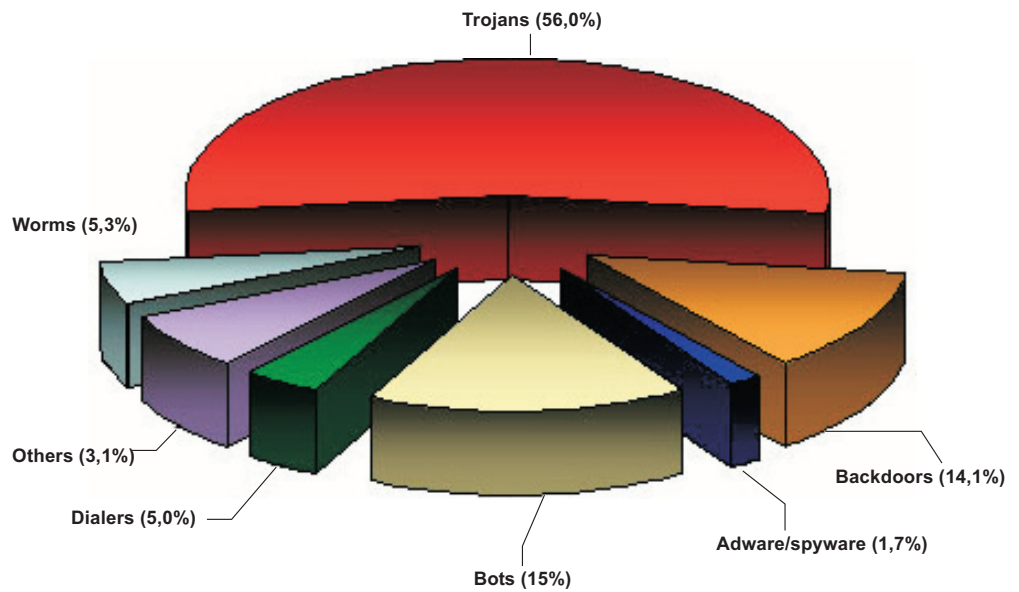


Figure 1. New Variants Detected for all Malware Types

The trends of previous quarters are still apparent. Trojans continue to be the malware type with the highest number of variants. The following graph shows data from the first three quarters of 2006:

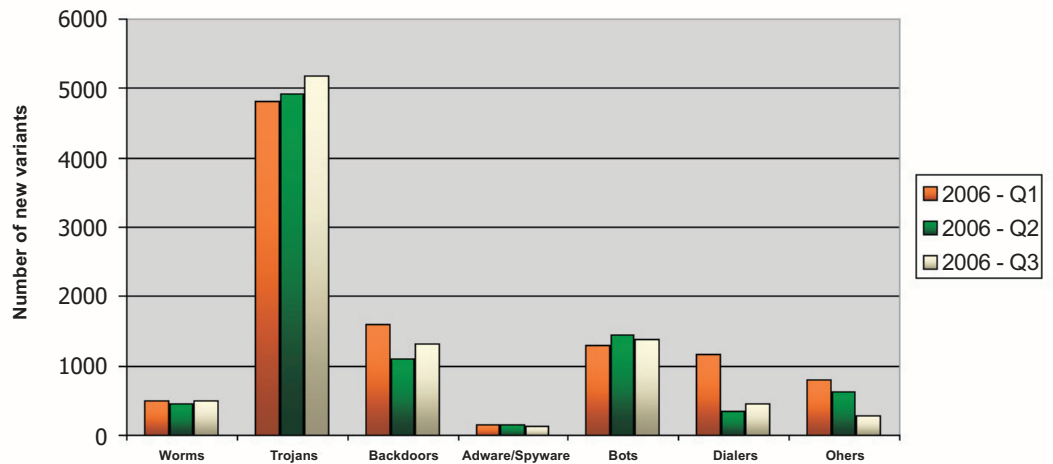


Figure 2. Number of New Variants which Appeared during the First Three Quarters of 2006

As the graph shows, the number of new variants of Trojans continues to rise. Not only are there more Trojans than any other type of malware, but they also continue to gradually increase their dominance over other malware applications, especially when compared with categories which are in sharp decline, such as viruses, potentially unwanted programs, hacking tools, etc.

Unlike other malware types (worms, adware and spyware), the number of dialers has decreased since the first quarter. We hope that this category will become less and less frequent as broadband internet becomes more accessible and therefore more widespread.

Threats Detected by Panda ActiveScan

The following diagram shows the distribution of threats detected by Panda’s online tool ActiveScan throughout the third quarter of 2006.

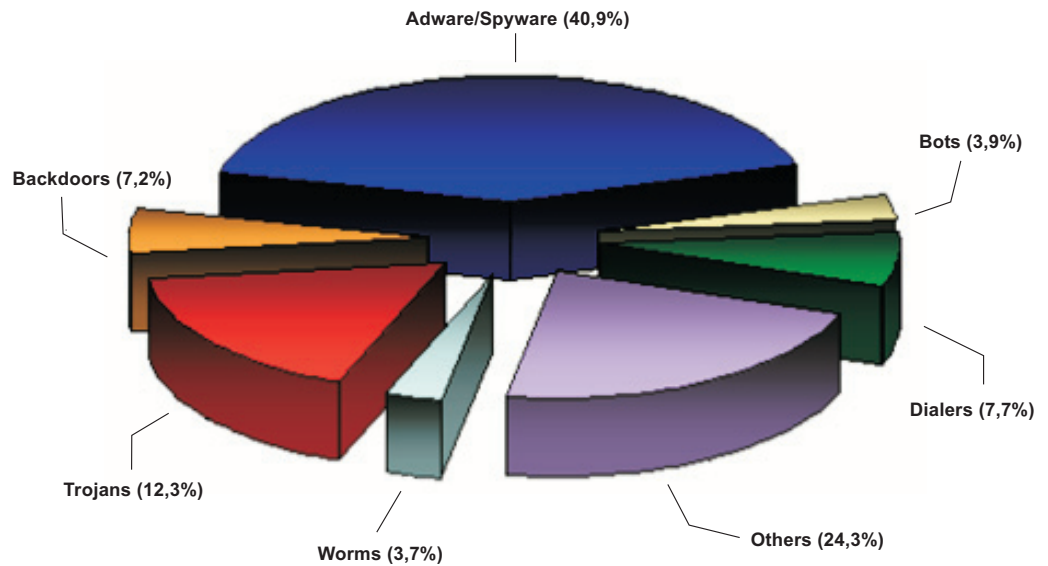


Figure 3. Types of Malware Detected by Panda ActiveScan

As in previous quarters, Adware and Spyware applications, despite representing only 1.5% of new variants, have been detected in almost 41% of computers scanned using the free online scanner Panda ActiveScan.

The following graph represents this quarter when compared with the previous two quarters of 2006.

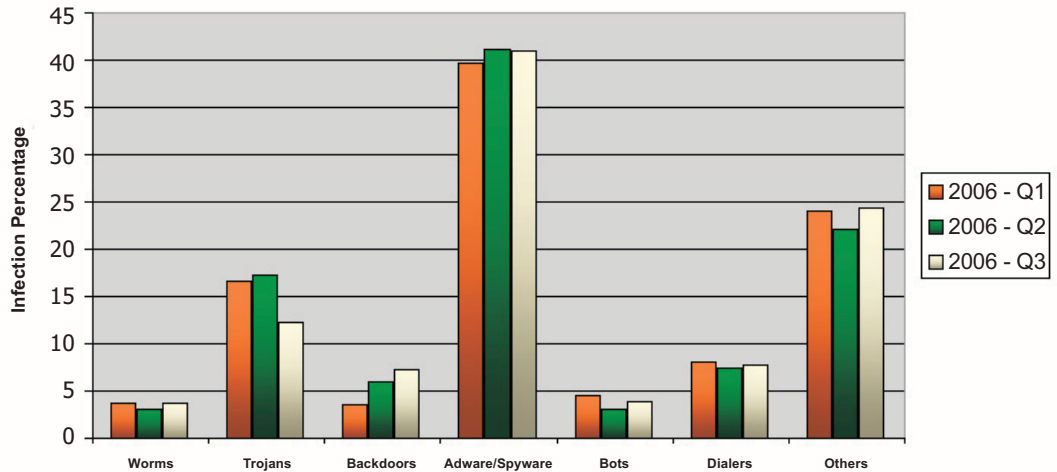


Figure 4. Figures for Each Type of Malware Detected by Panda ActiveScan during the First Three Quarters of 2006

No major conclusions can be reached from these figures. On the one hand, Spyware and Adware applications continue to affect the highest number of computers worldwide - around 40%. On the other hand, worms and bots continue to affect less than 5% of computers.

The number of Trojans detected has decreased by 5% since the previous quarter. However, this data is relative, given that the sum of applications associated with crimeware (Trojans, backdoors, adware, spyware and bots) continued to represent over 70% of all detections throughout the first three quarters of the year.



July – The Month of Browser Bugs

The security expert HD Moore is well-known for creating the Metasploit framework, an application which, in the words of its creator, aims to "provide useful information to people who perform penetration testing, IDS signature development and exploit research". Over the course of the last few months, Moore collaborated in the development of a series of "fuzzing tools" which led him to discover dozens of faults in the programming of various web browsers, making July 2006 the "month of browser bugs".

Fuzzing Tools, Errors and Vulnerabilities

Software validation using fuzz-testing involves systematically attaching the inputs of an application to a source of random data and taking note of the program's reaction. If the program crashes or another error occurs, then programming flaws are present.

These flaws are precisely the cause of exploitable vulnerabilities. In the most severe cases, these vulnerabilities can allow remote code execution (i.e. execution of a program with the same user permissions); other cases, which are not as severe but are still worrying, can result in denial of service attacks (making the application crash and close) or the disclosure of information.

By using this analysis technique on several web browsers, Moore discovered a series of defects which he published, with the precision of a Swiss watch, on a blog created specifically for that purpose.

Results Obtained and How to Interpret Them

The distribution of the 31 web browser errors published by Moore in his blog is shown in the table below:

Browser	Number of Errors
Internet Explorer	25
Firefox	2
Opera	1
Safari	2
Konqueror	1

Table 1. Distribution of Errors Found



The majority of errors in Internet Explorer (i.e. 22 of the total of 25) could be reproduced in version 6 of the application used on a computer with an updated version of Windows XP Service Pack 2.

A simple reading of Table 1 could lead you to believe that Internet Explorer is the most vulnerable web browser. Or that Internet Explorer only has 25 vulnerabilities. Or that the ratio of vulnerabilities in Internet Explorer to those in Firefox is 25 to 2. Or that Firefox, even though it only has 2 vulnerabilities, is twice as likely to be compromised as Konqueror.

However, remember that HD Moore's aim was not to show all the vulnerabilities present in the most popular web browsers, but to demonstrate how easy it is to discover these vulnerabilities using fuzz testing techniques. Needless to say, the browsers in question have more vulnerabilities than the ones published. Moore simply published a few vulnerabilities, one per day, throughout the month of July, but he could almost certainly have carried on for a longer period.

When considering Internet browser vulnerabilities, we cannot simply base our conclusions on the number of vulnerabilities alone. We must also take the following factors into consideration:

1. Characteristics of the vulnerability:
 - How serious it is (what can be achieved through its exploitation): arbitrary code execution, denial of service, disclosure of information, etc...
 - How difficult it is to exploit: this does not only mean the technical difficulties in finding useful code to exploit the vulnerability (which must be done only once), but also the defenses which can be used to protect it (e.g. firewalls).
 - How the vulnerability is exploited: can the vulnerability be exploited automatically by a malware application, or is user intervention required in order for exploitation to occur? For example, compare the vulnerability in RPC-DCOM exploited by the Blaster worm with the vulnerability in WMF files. The two vulnerabilities are equally serious as both permit arbitrary code execution, but the RPC-DCOM vulnerability does not require user intervention and only needs an Internet connection.
2. It is also important to bear in mind how widely each web browser is used. Logically, the characteristics of a vulnerability are not affected by the number of people who use the vulnerable application. However, the more users a program has, the greater the potential financial gains for a cyber-crook: with just one exploit a larger number of computers can be compromised.
3. Finally, another factor to consider is the length of time during which users are exposed to the vulnerability. How long does it take the manufacturer to provide a patch once a fault has been discovered?

By taking into account all these factors it is possible to interpret correctly the results obtained by Moore and not just look at the raw numbers.



Informing Users about Vulnerabilities

One of the recurring themes when discussing vulnerabilities is the way in which the general public is informed of them. There are various ways to deal with this problem:

1. **Security through obscurity:**
This method aims to offer security based on the fact that the system is not well known: even though manufacturers admit to the fact that vulnerabilities are present, they are unknown or difficult to find and as a result exploits cannot be developed for them.
2. **Full disclosure:**
Using this model, the full details of the vulnerability as well as how to detect and exploit it are revealed publicly before the manufacturer itself has been informed. This is the direct opposite of the "security through obscurity" model.

Theoretically, full disclosure should mean that the period of exposure to the vulnerability is shorter because the manufacturer will try to solve the problem as soon as possible in order to improve its image.

This method is the subject of some controversy because publicly revealing the vulnerability before a solution to it has been found could make it easier to exploit and therefore exploitation would be more widespread.

3. **Responsible disclosure:**
This method consists of informing the application manufacturer of the vulnerability before revealing it publicly. In this way, the manufacturer is given time to solve the vulnerability and offer a patch to affected users.

However, there is a risk that the manufacturer, realizing that the vulnerability has not been made public, will delay its response indefinitely. For this reason, manufacturers are usually given a previously agreed fixed-time period (e.g. 30 days). At the end of this time period full disclosure will occur.

Logically, each of these models has its supporters and opponents. Usually, IT security experts are in favor of either responsible or full disclosure. However, some manufacturers defend the "security through obscurity" method, and some prefer responsible disclosure.

At least 9 of the 25 vulnerabilities detected by Moore in Internet Explorer were disclosed to Microsoft in March 2006 but the company played the incident down by saying that the majority of faults could only be used to cause an error and close the browser application. However, at least one of these nine errors (which affected the ActiveX control hhctrl.ocx) was categorized by the security company Secunia as extremely critical and later resolved by Microsoft through the publication of its regular security bulletin on the August 8.

Reactions to the Month of Browser Bugs

Without a doubt, HD Moore's initiative highlighted a situation which was already at its peak. In some circles, the project was not received particularly well.

A clear and typical example of a manufacturer's reaction is that of Microsoft. The company complained about the fact that Moore disclosed the vulnerabilities publicly before updates were available so that users could protect their computers.



However, it is perhaps more surprising to hear of complaints from the cyber-crooks themselves.

After a week of writing in his blog, Moore began to receive email messages from Russia. A cyber-crook was complaining that a vulnerability he had been using unnoticed to hack computers had been revealed. When the vulnerability was made public, it would be resolved, meaning that the crook could not make such high profits from it.

This is food for thought. Cyber-crooks are not pleased when some vulnerabilities are made public. In fact, the reaction of the Russian cyber-crook serves only to confirm the existence of a shadowy panorama: a whole series of vulnerabilities are present in web browsers (and by extension in other applications) which have still not been dealt with by manufacturers or by security companies. These vulnerabilities are being actively, but silently, exploited by cyber-crooks in order to gain control of computers belonging to users all over the world.

When you think of it from that point of view, the Month of Browser Bugs initiative, although criticized by Microsoft, has proved to be what its creator claimed from the beginning: a way to expose the types of vulnerabilities found in web browsers today, as well as the tools used to find them.

Repercussions

The Month of Browser Bugs was not a merely anecdotal project. The vulnerabilities found were not mere proofs of concept, exploitable only within a controlled environment.

In order to illustrate this point, consider error number 19 on HD Moore's list: `WebViewFolderIcon setSlice`.

Although at the time this vulnerability was categorized as a denial of service, on September 27 an exploit was detected which was using the ActiveX `WebViewFolderIcon` control `setSlice()` method to execute arbitrary code. In this way, users were exposed to a new zero-day attack and Microsoft had to use all possible means to provide its customers with a solution.

The patch for this vulnerability was made available in the regular security bulletin for the month of October.

Conclusions

The harsh reality is that all web browsers, and by extension all computer applications, are vulnerable. No browser is error-free and completely invulnerable or unhackable.

Internauts should be warned: users of web browsers which have not traditionally been the object of attacks because they are not widely used could be feeling a false sense of security. These users may also not be used to regularly applying security patches.

As a result, although a relatively small number of vulnerabilities were detected by HD Moore in these programs, Firefox, Opera, Konqueror and Safari users should be alert (although they should not become paranoid). After all, a single unpatched vulnerability is all that it takes to compromise a computer. Your only line of defense cannot be the fact that you belong to a relative minority which, up until now, has not been a profitable target.

Vulnerabilities in Microsoft PowerPoint

Just one day after the publication of Microsoft's July security bulletin, we began to become aware of a vulnerability in PowerPoint which allowed arbitrary code execution in the vulnerable computer. All users needed to do to execute this code was to open a malicious presentation created for this purpose.

Attack of the Malicious Presentation

The first signs of a vulnerability were noticed around July 12, when email messages with an attachment containing a PowerPoint presentation were received. This presentation, written in Chinese characters, contained disrespectful comments about relationships between men and women.

Humorous gems such as "What is being romantic? Sending 999 roses to a woman who doesn't like you. What is being wasteful? Sending 999 roses to a woman who does like you" distracted the user while the presentation used a vulnerability to silently install a backdoor which was detected by Panda Software and identified as Bifrose.QN.

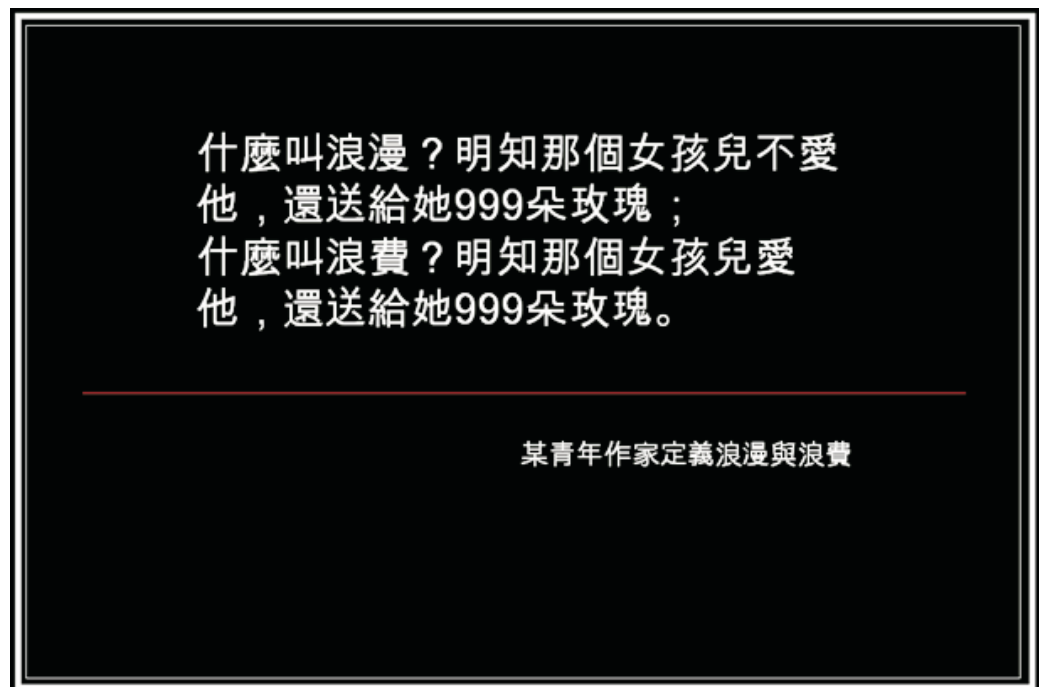


Figure 5. Example of One of the Slides in the Malicious Presentation

The backdoor opened several ports and waited for remote commands about what to do to the infected computer in the same way as a bot.



As mentioned above, the method of entry for this malicious presentation was an email message. However, the presentation was not sent out in bulk but targeted specific users, i.e. the message was sent to a small group of people but was highly personalized so that its recipients were more likely to be taken in by it.

Details of the Vulnerability

The vulnerability, which was unknown until the attacks were detected, was caused by errors when PowerPoint processed malicious presentations. The component affected was the MSO.DLL library which is shared by several Office applications.

The vulnerability allowed execution of arbitrary code using the same permissions as the user who had signed in (if the user had administrator permissions the potential damage would be much greater). Several PowerPoint versions were affected: Office 2003, 2002 and 2000 for Windows, as well as Office X and 2004 for Mac.

In order to exploit the vulnerability, a presentation which met a series of characteristics was created and distributed to vulnerable users. Although the most usual method of distribution is to send files of this type via email (because it is fast and cheap if botnets are used), other methods could also have been used: web pages hosting the presentation, P2P networks used for file sharing etc...

The Microsoft Security bulletin published for this problem was assigned the number MS06-048 and entitled "Vulnerabilities in Microsoft Office Could Allow Remote Code Execution".

A Certain Feeling of Déjà Vu

This is your last chance. After this, there is no turning back. If you take the blue pill, this section will end here; if you take the red pill, we will show you how deep the rabbit hole goes. The red pill? Well, don't say we didn't warn you.

Table 2 shows the timelines of several vulnerabilities discovered in Office applications over the last few months:

Regular Publication of Security Bulletin	Application	Zero Day*	Date of Solution	Days without Patch
05/09/06	Word	05/19/06	06/13/06	26
06/13/06	Excel	06/16/06	07/11/06	26
07/11/06	PowerPoint	07/13/06	08/08/06	27

* Zero day is defined as the first day during which the vulnerability is detected, even if it may have been exploited before that date.

Table 2. Dates of Security Bulletins and Discovery of Zero-Day Vulnerabilities in Office Applications



If you have a feeling of déjà vu, don't worry: it is just a fault in the Matrix. Or maybe it's just that the similarities between the three cases are frightening:

- The vulnerability is first exploited a few days after the regular publication of the Microsoft Security Bulletin. In this way, the vulnerability can be used for the maximum period of time before a solution is released. This means that it can be exploited freely and without punishment.
- The vulnerability is in a widely-used computer office application. The file types under attack are difficult to filter (filtering usually results in loss of legitimate information along the way) and they inspire greater confidence in users; this is because executable files have, over time, come to be considered as files which cannot be trusted blindly. Office documents, on the other hand, have seemed to offer greater security guarantees ever since the era of macro viruses came to an end.
- The vulnerability is used for targeted attacks, not for indiscriminate ones. The attack does not draw unwanted attention from computer security companies.

Don't Go Yet, There's More

Vulnerabilities in PowerPoint during this third quarter were not limited to the case described above.

On September 27, Microsoft published a new security warning, alerting users to a new PowerPoint vulnerability which also allowed execution of arbitrary code and which was again being used via targeted attacks.

This vulnerability was corrected in bulletin MS06-058 published on October 10.

Conclusions

The following months will be crucial in order to confirm the trend which is suggested here. We may be facing a constantly escalating war, similar to the one which came to an end some time ago between malware creators and computer security companies.

However, the time scale of this potential new war is completely different. While malware detection usually takes hours or at the most a few days, the normal time required to publish a Microsoft Security Bulletin is almost a month because of the decision to publish security bulletins on the second Tuesday of each month (although it is also true that, for more problematic vulnerabilities, Microsoft has taken the decision to publish an unscheduled bulletin, e.g. in the case of the vulnerability in WMF files). As a result, users are exposed to these vulnerabilities for at least a month.

The question is, if this trend is confirmed as others have been in the past in the world of malware, should Microsoft change its patch publication policy? Logically, the answer can only be "yes".



End of Support Phase for Windows Millennium and Windows 98

On the July 11, the same day that the monthly patches were released, Microsoft ended the extended support phase for Windows 98, Windows 98 Second Edition (SE) and Windows Millennium. Although this phase was meant to come to an end in January 2004, Microsoft decided to extend it so that more customers, both home and business users, would have enough time to change to more recent versions of the operating system.

An Unpromising Start for Windows 98

On the April 20, 1998, at the Comdex convention in Chicago, Bill Gates presented Windows 98, the newest version of his operating system at the time, to the public. However, the program was set to play a dirty trick on him.

When Chris Capossella, who was helping Gates with the presentation, tried to connect a scanner, the operating system decided to display the infamous blue screen of death which appears when the system is unable to recover from a system error. After deafening applause and laughter from the audience, Bill Gates smiled and said "This must be why we're not shipping Windows 98 yet". The show must go on after all.

Windows 98 was released on June 25, 1998. New features offered in Windows 98 which were not present in its predecessor, Windows 95, included system support for FAT32 files, USB drivers, the ability to control various monitors, AGP (Accelerated Graphics Port), etc...

The subsequent version, Windows 98 SE, corrected several errors and also included Internet Explorer 5.0, NetMeeting 3.0 and ICS (Internet Connection Sharing), which allowed several computers in a network to share the same Internet connection.

Both versions of Windows 98 were well received by the general public. According to data from Google for November 2003, 27% of web pages visited were accessed using these versions of the Microsoft operating system.

Windows Me - Criticized and Short-lived

Windows Millennium, which was launched on September 14, 2000, had the shortest lifespan of all Windows operating systems. Just one year after its release it was replaced by Windows XP, which has now been in use for over five years.

Windows Millennium included Internet Explorer 5.5 and incorporated many new features, such as automatic updates, Universal Plug and Play support (UPnP), System Restore and File System Protection.

However, the system was heavily criticized due to a wide variety of problems: instability, incompatibility with some hardware components, installation problems, etc...



Implications of the End of the Extended Support Phase

The end of the extended support phase for Windows 98 and Windows Millennium has one direct consequence: no more security patches will be released for these operating systems.

The following table give details of the different phases of technical support for these systems:

Version	General Release	End of Mainstream Technical Support Phase	End of Extended Technical Support Phase
Windows 98	06/30/1998	06/30/2002	07/11/2006
Windows 98 SE	06/30/1999	06/30/2002	07/11/2006
Windows Millenium	12/31/2000	12/31/2003	07/11/2006

Table 3. Key Dates in the Lifecycle of Windows 98 and Windows Millennium

What is the difference between mainstream technical support and extended technical support? There are three advantages of the mainstream technical support phase: no-charge incident support, warranty claims and new product design and features.

However, the main difference between the two phases lies elsewhere: Microsoft defines a difference between a critical vulnerability (which allows propagation of an Internet worm without user intervention) and an important vulnerability (which allows a computer to be compromised but requires explicit user intervention).

During the extended support phase, Microsoft provided users with updates via Windows Updates to protect their systems from critical vulnerabilities affecting Windows 98 and Windows Millennium. However, solutions were not provided for vulnerabilities classified as important. For example, the famous WMF vulnerability is not considered critical for these systems and therefore no solution has been found.

This will continue to happen with all vulnerabilities which come to the fore from the July 11 onwards. As a result, Windows 98 and Windows Millennium will continue to have the same level of security as they had on that date and will not benefit from updates which deal with pre-existing vulnerabilities discovered after that date.

Microsoft claims that this method has been selected for security reasons. As these products are out-of-date and could present a security risk, Microsoft recommends updating to a newer and more secure Windows operating system (a very ironic claim indeed). Today, Microsoft recommends the use of Windows XP, the most recent commercially-released system. However, with the upcoming release of Windows Vista and all the marketing material claiming that it is the most secure operating system to date, it is pretty clear what Bill Gates' company will be recommending next.

Statistically, the number of users affected by this Microsoft decision worldwide is approximately 70 million, a far from negligible figure at first glance, but one which represents a mere 13% of all registered Windows users.



Conclusions

Should we abandon discontinued operating systems or protect them? That is the question.

Some companies believe that the end of the Windows 98 and Millennium support phase does not mean that they will become the preferred targets of cyber-crooks. However, the problem lies in the fact that these systems could share vulnerabilities with other, more recent Windows operating systems which are under attack and which still benefit from security updates.

If you need to keep Windows 98 or Millennium installed on your computer (if, for example, the computer does not meet the minimum hardware requirements for installing a newer system), you must follow the basic rules of computer security: keep your antivirus application updated and active at all times, use a firewall, make regular backup copies and keep up-to-date with developments in malware.



MySpace in the Line of Fire

As mentioned in the previous PandaLabs report regarding the second quarter of 2006, "when an Internet company stands out it will attract the attention of cyber-crooks". At that time the social network MySpace was the fifth most visited site worldwide. During this third quarter it has moved up a place and is now positioned just behind Google.

Those Who Cannot Remember the Past are Condemned to Repeat It

Fasten your seatbelts and return your seat to the upright position. We are about to begin a journey back in time so that we can put the present into context. Ready?

We're here. As the mist begins to clear, it is the beginning of October 2005 and we are in Los Angeles, USA (make sure you do not interfere with anything that's going on, it could have unforeseen consequences in our own time). A 19 year-old man named Samy is pondering how to make himself popular amongst his MySpace friends and wants to edit his profile without the restrictions imposed by the website. Using his knowledge of JavaScript, and by studying how MySpace imposes the restrictions, he quickly discovers how to do something a lot more... far-reaching.

He does not stop at automatically adding himself to the friend lists on other profiles without asking for permission. He also adds a phrase ("but, most of all, Samy is my hero") to the "Interests" section of every profile that visits his own profile or which visits profiles which have visited his own. This results in a propagation technique worthy of a biological virus. It infects the people closest to him who, in turn, infect the people around them...

For those of us who like statistics, in 20 hours Samy managed to add his name to the friend lists of over a million profiles.

After this, MySpace was out of service for several hours while the MySpace team carried out "maintenance work".

Let's come back to the third quarter of 2006. On our way we can look at a brief summary of what we have seen: by taking advantage of the profile personalization feature, getting round the restrictions imposed by the page itself and using JavaScript knowledge, a young man was able to create a code capable of propagating itself in MySpace profiles and carrying out actions which in principle only the owner of a profile should be able to carry out. We could call this a MySpace worm.

Now we have arrived back to the July 16, 2006 which is when reports began to be made about problems with Shockwave Flash files in MySpace. Those who visited the infected profiles had their own profile infected, and were redirected to a page with political content which explains one of many conspiracy theories claiming that the United States government was behind the terrorist attacks which took place on the September 11, 2001.

When a MySpace user visited an infected profile, an embedded Flash object named `redirect.swf` would redirect the browser to another web address in which a second Flash object was embedded (`retrievecookie.swf`). This Flash object retrieved the information required to access the profile and then modified it to include the Flash file which set the whole process in motion again.



This is another case of a code capable of replicating itself in other profiles through a simple visit to an infected profile. Although the method used was different, the result was always the same as in the Samy case.

Even though the effects of this Flash worm were merely anecdotal, the code could clearly be made malicious with just a few modifications. In addition to this, in the months leading up to the appearance of this worm a similar technique had been used to illegally gain access to MySpace profiles.

MySpace issued a memo regarding this matter stating that it was possible to avoid being affected by this worm by installing Adobe Flash Player version 9. However, the web page did not tell users how to get rid of the worm once a profile had been infected (editing the profile and deleting a specific line).

A MySpace Banner Distributes Malware amongst Users

A few months ago, we played a practical joke on a colleague who was in charge of writing press releases. We called him on the phone and tried to make him believe a story which, had it been true, could make your hair stand on end. The story we wanted him to believe was that somebody had managed to compromise the Google homepage and had inserted an image which exploited the WMF vulnerability in order to distribute malware to all users of the search engine. Obviously our colleague did not believe us.

However, having seen what happened a few weeks later (on the same day as the Flash worm to be exact, which was really bad luck), we could not help but think that it was lucky we were not overcome by the dark side of the force.

According to an analyst working for the security company iDefense, the threat took the form of an innocent advertisement for patio furniture which appeared while users browsed MySpace. Suddenly, the following warning appeared: "You have chosen to open exp.wmf, which is a binary file. What should Firefox do with it?"

Do you remember the case of the WMF vulnerability? This was described in the first quarterly report of 2006. A vulnerability in the GDI32.DLL library used by, amongst other programs, Internet Explorer, allowed execution of arbitrary code. The seriousness of this vulnerability and its intensive exploitation on the Internet meant that Microsoft had to release an unscheduled patch in January 2006.

So the WMF monster reared its ugly head again. Perhaps it never went away in the first place.

If this malicious advertisement was shown on an unpatched Internet Explorer browser, the vulnerability was used to install a Trojan on the computer which would then install adware programs belonging to the PurityScan family. The effects of this adware ranged from the appearance of an enormous number of pop-up advertisements to the recording of the user's browsing habits.

How did this threat reach MySpace? Via the company which provides the advertisements shown on its pages, which also supplies advertisements on many other websites. The advertisement in question would have been present on MySpace since the July 8 (i.e. 8 days before the first infection was reported).

Hemanshu Nigam, CTO (Chief Technical Officer) of MySpace, stated that the incident was a criminal act and that the problem lay with the company that supplied the advertisements. He also urged users to follow basic security practices (antivirus and anti-spyware applications, patches). He added, "if users have applied the simple patch available from Microsoft.com, they will not be vulnerable to this criminal act".



As Mr Nigam suggests, as Internet users, we are easily led like sheep. When this happened on MySpace, a patch for the WMF vulnerability had been available for over 6 months (and, worst of all, we can bet that there are still users whose computers are being compromised right now because of this vulnerability). So yes, we are all sheep for not applying the patch, and for not protecting ourselves well enough using basic security measures. Also for blindly trusting that MySpace would analyze the content provided by advertising companies, and for believing that the site checked that advertisements appearing on its pages were not used to distribute malware amongst all its sheeplike visitors.

If we are going to count sheep, we will have to know how to count up to a million. One server used to count how many times the malicious program had been installed counted 1,000,000 affected users.

Conclusions

We can say it louder, but not any clearer. Download and install the patch for the WMF vulnerability. Now! (If you have to, stop reading this report, we would rather you did).

Keep up to date about vulnerabilities present in the programs you use and apply the necessary patches. Each and every time. We know it is hard work but, like any work, it has its rewards.



The strange case of the MS06-042 patch

August 8 fell on the second Tuesday of the month. The regular bulletin publication cycle came with 12 patches under its arm this time. The cumulative update of Internet Explorer, identified as MS06-042, was to become the unexpected star of a drama all of its own.

Accumulation of vulnerabilities

The MS06-042 security bulletin resolved a total of eight vulnerabilities in the Microsoft web browser:

1. Cross-domain information disclosure.
2. HTML layout and positioning memory corruption.
3. CSS memory corruption.
4. HTML rendering memory corruption.
5. COM object instantiation memory corruption.
6. Source element cross-domain vulnerability.
7. Window location information disclosure.
8. FTP server command injection.

In these cases, the vulnerabilities were exploited as per usual: convincing users to visit a specially-crafted website. If a user accessed a malicious website via a version of Internet Explorer that had not been updated, the computer was automatically compromised.

The overall seriousness of these eight vulnerabilities was **Critical** for all active Microsoft operating systems (Windows 2000, Windows XP and Windows Server 2003), meaning that it was recommended to install the patch immediately. It's safe to say that more than a few people regretted following this advice.

Something stinks with the MS06-042 patch

Just three short days later, Microsoft had to publish an article on its Knowledge Base, alerting users of the fact that Internet Explorer 6 (with Service Pack 1 installed) operating on Windows 2000 (Service Pack 4) or Windows XP (Service Pack 1) may unexpectedly crash after installation of the MS06-042 patch, when certain websites were visited.

In other words: after installing the MS06-042 patch, a group of specific users would experience Denial of Service problems when online. These problems would arise when they were trying to access a web Server that used HTTP v1.1 compression.

The Knowledge Base article referred to a patch that would be able to solve the problem. However, the problem was that this solution was only available through Product Support Services, and was not made public on the website.



A solution that introduced new critical vulnerabilities

In the wake of the vulnerabilities introduced by the patch, and given the scope of its impact, a huge number of discussions went on in companies, forums and mailing lists, all related to IT security. Finally, the renowned eEye research team decided to investigate the problem a little deeper, eventually finding out that the repeated crashing of Internet Explorer installed on specific operating systems was due to a buffer overflow.

In other words, the problem was not just about a browser that suddenly closed, but one which could also be exploited to run malware on the vulnerable computer: we were faced with a security patch that could introduce a critical vulnerability.

eEye worked together with Microsoft, allowing them to have all the information they needed, plan their strategy, etc. Finally, Microsoft agreed to launch a new version of the MS06-042 patch on August 22, meaning that eEye could also inform users of the dangers represented by the original patch.

And again and again!

However, when it came to the 22nd, instead of a new patch appearing, Microsoft published a new security alert.

It seemed that the new patch had not passed the strict quality control tests imposed by the Microsoft software factory, which meant that its publication would have to be delayed.

Or at least that was the story that was made public. According to information that was released by eEye at a later date, the true problem lay with one of the Microsoft patch distribution systems. Therefore, instead of making the patch available through other means (for example, Automatic Updates, accessible via the Control Panel), it was decided instead to postpone its publication.

Faced with this action, eEye decided to also publish a warning alerting users about the vulnerability, so that they were informed about the risks involved and possible counter-measures.

Immediately afterwards, Microsoft published a new security alert, warning that "long URLs to sites using HTTP v1.1 and compression could cause Internet Explorer 6 with Service Pack 1 to unexpectedly exit".

OK – let's take a deep breath and go back over the facts – this is all a little long-winded, even for a typical Microsoft title. eEye warns of a vulnerability. Microsoft alerts users about the same vulnerability and clearly indicates where it should be looked for: in long URLs. It's just like putting up a poster that says: "here's the vulnerability, feel free to come and get it". What's more, on the official Internet Explorer blog, one of the programmers posted the target on the URLMON.DLL library. Since when have clues as useful as these been made available for those seeking to exploit vulnerabilities? After this came the subsequent media declarations against total disclosure, clearly referring to the role played by eEye, and in favor of responsible disclosure: eEye's alert did not contain information that was as dangerous as that contained in the Microsoft alert.

Finally, a few days later on the 25th, Microsoft published the new version of the MS06-042 patch. In the acknowledgements section of the edited bulletin, the name of eEye was conspicuous by its absence, despite the fact that this was the organization which had initially informed Microsoft of the matter.



Third time lucky

But wait – there's more! This drama still has one final chapter: the MS06-042 bulletin had to be edited for a third time.

Feelings of déjà-vu were starting to become unbearable: eEye discovered that those excessively long website addresses for pages that use HTTP version 1.1 and support compression caused an error that allowed the execution of arbitrary code. Despite similarities, this was a totally new vulnerability, introduced by the second version of the patch.

In this way, on September 12, on the very day set within the regular cycle for the publication of patches, Microsoft once again updated the MS06-042 bulletin, once again urging all users to install the updated patch.

Is all that clear? Apply the MS06-042 patch launched on September 12 to solve the critical vulnerability introduced by the MS06-042 patch on August 25, which corrected the critical vulnerability caused by the installation of patch MS06-042 published on August 8 which, in turn, corrected 8 vulnerabilities which had been classified as critical.

As a final twist in the tale, the (until now) latest edition of the MS06-042 bulletin saw Microsoft explicitly thanking eEye for their collaboration in letting Microsoft know of the issue of buffer overflow in long URLs.

Conclusions

If to err is human, then sweeping the dust under the rug is even more so.

Finding an error in a patch that aims to solve vulnerabilities is not something that we should get stressed out about. It's not the first time that a new version of a specific application has included vulnerabilities solved in the former version.

On the contrary, what this should do is teach us more about the nature of this cat-and-mouse game between vulnerabilities and their solutions. In addition, it should teach us about the reaction from the various players in the game.

With eEye we have an agent that investigates vulnerabilities and informs about those it finds. In this specific case, eEye's disclosure, despite the fact it did not follow Microsoft plans, was far from being irresponsible.

In the events surrounding the MS06-042 bulletin, Microsoft was well and truly beaten. However, this loss was not down to the errors in the published patch, but had more to do with the posture the company adopted. They postponed the release of the patch which had been scheduled for August 22, not because of the solution's quality, but because of technical problems which had nothing to do with the solution itself. They also published information that gave tempting clues to anyone who was interested in looking for ways to exploit the vulnerability. Not only that, but they failed to clearly explain how urgent it was to apply the MS06-042 patch on September 12, treating it instead as a normal re-editing of a solution.

To illustrate this, all you have to do is ask yourself the following series of questions: Did you install the original MS06-042 patch? If so, did you apply the correction issued on August 25? If so, did you install the definitive patch? (Obviously, if your reply was "No" in all three cases, what are you waiting for? All you have to do is install the latest version).

After the patches, then comes the malware

As we already mentioned in this report, the events of recent months suggest that IT criminals are using the days leading up to the second Tuesday of the month to unveil to society in general the latest vulnerabilities they have detected, beginning to exploit them immediately.

However, there is an additional trend associated with the regular cycle of Microsoft security bulletin publications: the appearance of malware that exploits some of these latest patched vulnerabilities.

The MS06-040 Bulletin

This bulletin was published on August 8, along with 11 other bulletins, and was categorized as critical. It dealt with the possibility of causing a buffer overflow in the Server service, so that arbitrary code could subsequently be executed. In other words, this represented complete control of the computer.

The systems affected by this vulnerability were Windows 2000, Windows XP and Windows Server 2003. However, as the bulletin clearly stated, those computers operating on Windows 2000 were most at risk.

As far as the way in which the vulnerability was exploited, this really should be looked at with a critical eye. By simply sending a specially-created network packet, code could subsequently be executed. Do you remember the cases of the Blaster and Sasser worms? These incidents had serious repercussions, both in August 2003 (Blaster) and in May 2004 (Sasser). Many users can probably still remember the famous dialog box that showed a 60-second countdown until the computer restarted.

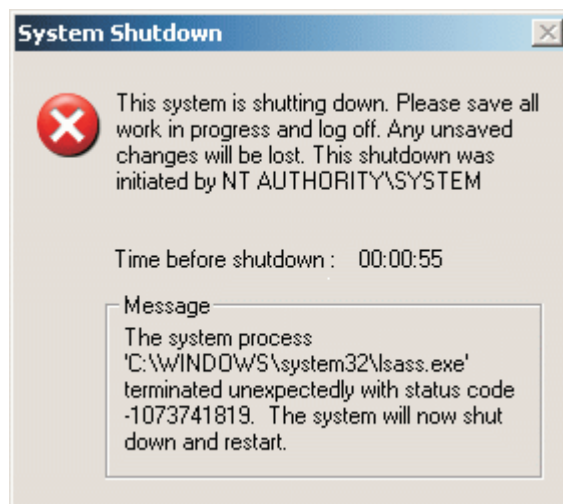


Figure 6: The countdown displayed by Sasser



At least in theory, the vulnerability that had been corrected by the MS06-040 bulletin had all the signs of becoming the distribution vector for the next worm to spread by mass propagation. This led several security experts to take advantage of the imminent advent of a critical threat (once again scurrying around, gathering stores and hiding underground, as happened with Tearec.A). Others, on the other hand, decided that the situation was not so serious, and that all that needed to be done was to apply the patch and carry on as normal.

First public sighting: Oscarbot.KD

Strictly speaking, the vulnerability was already in active use before the publication of the bulletin. In fact, in the bulletin's Frequently Asked Questions section, Microsoft admitted having reports that substantiated this. Once again, the vulnerability had not merited general attention because it had been used in targeted attacks.

After the appearance of various public exploits and the release of the patch, (on which the process of reverse-engineering can be used in order to obtain the necessary information to obtain a useful exploit), it was not long before the first sighting of malware exploiting the vulnerability appeared.

During the last few hours of August 12 (in other words, four days after the patch was released), reports began to be received on the appearance of the Oscarbot.KD bot. In addition to propagating through instant messaging programs and shared network resources, it also exploited the MS06-040 vulnerability.

This was the only characteristic that made this particular malware special. As for its other effects, well these were as to be expected: disabling of the Windows XP Security Center and firewall, receipt of remote control orders via IRC, use of file and service names related to Microsoft (such as Windows Genuine Advantage) to throw the user off the scent, etc.

Despite initial predictions, this first malware to exploit the MS06-040 vulnerability had an extremely low level of incidents. At the point at which Oscarbot.KD activity was at its highest, Panda ActiveScan only detected that 0.13% computers were affected, a figure which rapidly decreased.

Onwards and Upwards

Evolution has always awarded those beings which adapt best to their surroundings. The reward on offer is the survival of the individual, and the continuity of its kind. What relationship exists between this theory of evolution and the world of malware?

The best place to observe this parallel is through the evolution experienced by bots, from their origin up to the present day. More specifically, it is important to look at the methods they use to propagate to other computers. Let's use as an example one of the primitive varieties of the family of bots which has been most widespread to the present day: Gaobot.

Its Gaobot.L variant (which appeared in September 2003) used various means of propagation:

1. Shared network resources..
2. Exploiting vulnerabilities: RPC-DCOM, WebDav.



Less than one year later, in August 2004, Gaobot.AIR was detected, with the following means of propagation:

1. Shared network resources.
2. Exploiting vulnerabilities: RPC-DCOM, WebDav, LSASS.
3. Computers compromised by other malware: Bagle.A, Mydoom.A, etc.
4. Computers with specific applications installed: DameWare Mini Remote Control, SQL Server, etc.

At the start of this year, Gaobot.LTL used everything, except tom-toms and postal mail, methods which will no doubt be available on future variants:

1. Shared network resources.
2. Exploiting vulnerabilities: RPC-DCOM, WebDav, LSASS, UPnP.
3. Computers with specific applications installed: DameWare Mini Remote Control, SQL Server, etc.
4. P2P Programs.
5. Instant messaging programs.
6. E-mail.

And now, an easy question. Guess which is the latest propagation method that Gaobots have incorporated into their arsenal? Yes, you're right: in the exploitation of vulnerabilities section, it is important to add the one relating to the MS06-040 vulnerability we talked about before.

Nevertheless, this is not the only family that has been adding its new variants that propagate through vulnerabilities. The range is rounded off with Aimbot, Sdbot, Spybot, etc. All these bot families are increasing their propagation methods through the most significant vulnerabilities that are being discovered each day.

A secondary shock: MS06-047

This, however, has not been the only recent example. Another bulletin published in August was the MS06-047, which detailed a vulnerability in Microsoft Visual Basic for applications (VBA), for Office 2000, Office XP, Works, etc.

A specially-created Office document that supports VBA (in other words, Word, Excel and PowerPoint, among others) could cause a buffer overflow that would allow for the execution of arbitrary code.

Around August 14, news spread of a malicious Word document that exploited this vulnerability. Its aim was to download new components (Trojans and backdoors) from various websites.

Conclusions

As far as the MS06-040 bulletin is concerned, where is the terrible blow that we were all expecting? Was all this worry stemming from the vulnerability simple an exaggeration by several experts? The tale of the boy who cried wolf undoubtedly springs to mind. However, it would be foolish to remain tied to such a simple analysis.



The vast majority of security companies are in agreement on the concept of crimeware which, in short, is malware designed to obtain fraudulent financial benefit. The message transmitted by all of them is homogeneous and unmistakable: mass epidemics are over, as are red alerts and media focus on a specific case. Today we are in the era of mass attacks, malware silently taking advantage of vulnerabilities, and zero-day attacks.

Within the dynamics of current malware, the Trojan or bot is the final component that aims to install itself on the computer. The exploitation of vulnerabilities, be these at zero-day or a few days before the publication of a security patch, continues to have a single aim: to install a malicious component in such a way as that it remains hidden, and therefore achieve the highest levels of performance possible. This performance is measured in terms of the number of computers infected, which can subsequently be evaluated in terms of economic performance.

Finally, let's highlight once again something which could seem ironic. In the specific case of the MS06-040 patch, both those experts who predicted the end of the universe as we know it with the dawning of the new millennium and those who were unfazed and saw no need for the cry of Apocalypse, agreed on one point: it is fundamental that you keep your operating system and applications up-to-the-minute in terms of security updates. After that, you can sit back and decide whether some experts are over-reacting or others are simply too laid back in the matter.



The Consumer Reports 5,500

In August a unanimous uproar could be heard from the vast majority of antivirus companies in protest at the study carried out by renowned magazine Consumer Reports. The object of their fury was not the result (as there are always winners and losers in every situation), but the way in which the analysis had been carried out: through the creation of 5,500 new types of malware.

A brief introduction to Consumer Reports

For those not in the know, Consumer Reports is an American monthly magazine, dedicated to the publication of service and product comparisons, (anything from cars to drugs), analyzed in the own testing bank.

The magazine enjoys great popularity in the USA, thanks to the quality of its analyses and a code of ethics that makes it largely independent from external commercial influences. To illustrate this point, consider the fact that, on the one hand the magazine does not have any advertising whatsoever, and on the other, the analyses are carried out on products that have been acquired in stores, and not on samples sent by the producers themselves.

Analyzing discord

After detecting its readers' need for an independent comparison to evaluate the effectiveness of antivirus programs, Consumer Reports decided to prepare a study for its September 2006 edition. This study would analyze the capacity of various products in tackling different malware, both known and totally new.

In order to do this, the magazine decided to rely on the collaboration of the IT security company ISE (Independent Security Evaluators), so that the tests carried out would reflect real conditions with the highest possible levels of accuracy. Not only was threat detection capacity going to be tested, but also other characteristics, such as false positives, update frequency and speed, ease of use, speed and additional tools included (scheduled analyses, instant message analysis, firewall, etc.).

As far as new threat detection is concerned, this can be based on various methods, including heuristic analysis and behavioral analysis. Now, how can all these technologies be tested? How is it possible to objectively calculate an antivirus' capacity to detect unknown malware, for which no signatures are currently available?

The response from Consumer Records was simple: to create 5,500 new types of malware, and subsequently study whether the products tested were able to detect them or not. These new types were based on six different families, the typical ones which can most easily be encountered during the typical activities of an Internet user.



It is not necessary and it is not useful...

The reactions from the antivirus companies did not take long to come, and deep down they were unanimous in their opinion: creating new malware samples in order to carry out a comparison of security programs was a crass error.

Despite the different ways of expressing themselves (for all those who said that they wanted to bang their heads off a brick wall – we hope you've recovered), the criticism was always the same: with the numbers of malware types already well exceeding 100,000, why was it necessary to add 5,500 new threats to this already dangerously high level?

In fact, the antivirus industry is strongly opposed to the creation of new malware samples, even when they are only being used to analyze their products. There is no danger that new malware may become extinct, as its numbers increase by some 250 on a daily basis.

Up to the present day, 155 signatures have been added to a public letter which claims that "it is not necessary and it is not useful to write computer viruses to learn how to protect against them". This is a declaration of principles that has been written by all manner of IT security professionals backed up by years of experience, from CEOs of antivirus manufacturers to independent researchers, and including consultants, software architects and many others.

To all the criticisms generated over the issue, which are already extremely powerful, two further considerations must be added. On the one hand, there ALREADY ARE independent bodies dedicated to carrying out comparisons of antivirus products: just look at Av-test.org, one of the most renowned organizations in this field and led by Andreas Marx, who has an excellent reputation.

On the other, there ALREADY IS a method to test antivirus programs and their ability to detect new threats. Up until now so-called "retrospective" analysis has been used on a general basis, which consists of testing an antivirus program which has gone for various weeks of months without updating its signatures, using current examples of malware. In other words, it tests the antivirus in a sort of "deferred future", putting it up against samples which, although not new in the strictest sense of the word, are unknown to the program.

Not a one-sided battle...

Not everyone agreed on automatically condemning Consumer Reports, however.

Jürgen Schmidt, for example, from Heise Security, mentioned an unspoken commandment agreed on between antivirus companies: "Thou shalt not create new viruses". Although he does recognize it as a sensible measure, he also claims that it is being used to launch attacks on certain independent studies. As well, he also spoke of a weakness suffered by retrospective analyses: the virus creators themselves.

We have already spoken about how, when it comes to IT security, having the largest market share makes a company a specific target, and this couldn't be any more true in this case. In fact, Schmidt talks of a highly well-known trial and error technique: before releasing a new type of malware, its creator carries out a test on the antivirus programs with the largest market share, modifying the version until the unknown threat detection module of these antiviruses is no longer capable of recognizing it.

When this point is reached the malware is fully developed, and the threat can immediately be released without any danger of it being detected from the word go, at least by the most widespread antivirus programs.



This also has a further impact: the larger the market share, the more driven the virus creators are to ensure that their creations pass by unnoticed, thus meaning they perform much more poorly in retrospective analyses.

From this point of view, it is possible to justify analyses through newly-generated malware samples, so that testing can remain independent from the market share of the antivirus being tested.

Conclusions

In theory, there is no chance of the 5,500 new viruses created by Consumer Reports being leaked to the Internet. The only copy of them is on a CD, and they have been tested in a controlled environment (in other words, they have been run in a virtual environment on a computer with no Internet connection). In this way, the indignation and outrage generated by this news may seem unnecessary.

However, the “Thou shalt not create new viruses” commandment, to which antivirus manufacturers implicitly adhere, is not arbitrary. It is born of a code of ethics, in the same way as other professions maintain similar codes to safeguard the privacy and confidentiality of their clients.

One of the urban legends surrounding antivirus manufacturers is that they themselves are the ones who create viruses, then setting out to try and “detect” them and therefore never being short of cash. However, these events have managed to dispel that myth. If we already have Consumer Reports, why would we bother having an army of evil programmers in the basement?



Google and malware

Throughout the quarter the good name of Google has been repeatedly associated with malware. Resolution of vulnerabilities, malware originating through searches, alerts against malicious websites, Trojans which disguise themselves as Google tools... All this makes up a particular collection of news items relating to malware on one of the most-widely used websites around the world.

Google solves a vulnerability in its RSS reader

At the beginning of July, in a blog on IT security, an announcement was made regarding the discovery of a cross-domain vulnerability in the RSS reader provided by Google (this same blog also referred to another characteristic which we will discuss in more detail later, the redirection from the google.com website to other domains).

The vulnerability's potential was found in the ability to host a phishing site on Google, with the aim of then stealing the session cookie, providing the necessary information to sign into Google services as a registered user and thereby compromise any information stored therein.

This vulnerability was made public following the line of complete disclosure: in other words, without advising Google of the situation beforehand.

The company was quick to react, however, and it was not long before the problem with the RSS reader had been rectified, eliminating the attack vector.

Google indexes executable files

Despite the fact that this characteristic came to light at the end of June, it wasn't until the start of the third quarter, in July, when it became the focus of great attention on various blogs, becoming *vox populi*.

If the string "Signature: 00004550", is entered into Google, the famous search engine can reference up to 192,000¹ different results, most of which belong to executable files.

In fact, the "Signature: 00004550" text string is found within the code for PE (Portable Executable) files, valid for 32-bit systems. In other words, EXE, DLL (Dynamic Link Library) and OBJ (Object Code) files.

The fact that Google offered diverse types of files within the results was more than well-known. However, the indexing of executable files was not such common knowledge.

¹ This number was later reduced by a significant amount, and also includes various references to blogs, articles and sites that refer to this piece of news.



Below is a table which contains the most normal file formats, as well as the type of file they represent:

Extension	File Type
PDF	Adobe Portable Document Format
PS	Adobe PostScript
WK1, WKS, WKU WK1, WK2, etc.	Lotus 1-2-3
LWP	Lotus WordPro
MW	MacWrite
XLS	Microsoft Excel
PPT	Microsoft PowerPoint
DOC	Microsoft Word
WKS, WPS, WDB	Microsoft Works
WRI	Microsoft Write
RTF	Rich text format
SWF	Shockwave Flash
ANS, TXT	Text

Table 4. File formats indexed by Google

In the past there had been talk of the possibility of using this characteristic to carry out searches for elements that could be used for malicious purposes: Excel spreadsheets with employee salaries, Word documents with password lists, etc. This content was indexed by Google and offered as part of search results, with the associated potential dangers to privacy and/or confidentiality.

However, another twist lies in the fact that it is also possible to obtain results relating to executable files, from which a certain percentage correspond to malicious executables.

In fact, a high number of results refer to spyware or adware, which were stored on malicious sites. In other cases, the sites were legitimate but had been compromised, so that they involuntarily took part in the distribution of this kind of malware.

And if that were not enough, it is also possible to find examples of viruses and worms in a more precise manner. For example, by discovering one of the internal strings of worms as famous as Bagle and Mydoom, (which can be easily obtained through IT security information websites), it is possible to find websites which still host files from some of the varieties of this family.

However, it is important to bear in mind that Google is not the only tool capable of being used to find executable files. Other search engines, such as MSN and Yahoo!, also offer a huge range of resources belonging to executable files when the same search is carried out.



The question to be asked is, therefore, why does Google index executable files? All signals seem to point towards the fact that the company wants to offer a search service that includes indexed files.

A Trojan disguised as a Google toolbar

On Wednesday, July 19, the circulation of an e-mail entitled “New Google Toolbar released” was detected.

Within these messages recipients found a link to a website which, in terms of both its URL and its appearance, could easily be confused with the legitimate Google download page. The false site offered the possibility of downloading a file called *GoogleToolbarFirefox.exe*.

As you can probably guess, this file was actually malware (a Trojan from the Ranky family, to be precise). Once executed, it turned the computer into a zombie under the control of a remote user, allowing all manner of criminal activities to take place. Although in the past it was more common to use denial of service attacks for other aims, this activity has currently been relegated to the backburner, in favor of others such as sending of spam, fraud on online payment systems, the installation of adware and spyware on infected computers, etc.

As regards the message itself, we can see that this is a classic case of social engineering. The attacking user wins over the confidence of the subject through:

- a) The use of a well-known “brand” like Google, as well as a well-known tool offered by that “brand”, which is widely available.
- b) The appearance of the website which has been accessed, copied from the original in such a way as to be practically indistinguishable.

This situation is further reinforced through the use of a redirection technique which is allowed by Google. More specifically, links like the following:

<http://www.google.com/url?q=http://www.pandasoftware.com>

direct the browser to:

<http://www.pandasoftware.com>

In this way, it is possible to take advantage of the trust felt by a relatively inexperienced user when they see that a link they are about to access starts with the character chain <http://www.google.com>, giving them peace of mind.

It is important to point out the fact that this characteristic is not exclusive to Google, but can also be found on other sites, including Altavista and Netscape.

Here it is useful to offer a piece of advice which, although it is repeated time and time again, still rings true: do not automatically trust links that you receive via email messages or instant messaging programs.

Google to warn of malicious sites

It is no stretch of the imagination to say that all Internet users, at one moment or another, have used a search engine. One of the most widely-used (which is actually permanently among the top 5 most visited websites) is Google. We all know the way Google works: each time that a user carries out a search, he or she is presented with a list of possible results that contain the keywords from the search, listed in accordance to a specific algorithm.

In theory, the results that are returned should never contain any moral judgment or recommendation in terms of the truthfulness or level of trust of the site in question. Each user is free to decide on the pros and cons of visiting any of the sites returned as a result of the search they have undertaken.

However, since the beginning of August Google has offered a new feature, aimed at helping users to protect themselves from potentially dangerous sites.

In fact, after carrying out a search, if a user decided to click on a link that will re-direct him or her to a dangerous site, they are first re-directed to an intermediary warning page.

Warning - the site you are about to visit may harm your computer!

You can learn more about malware and how to protect yourself at StopBadware.org.

Suggestions:

- ◆ Return to the previous page and pick another result.
- ◆ Try another search to find what you're looking for.

Or you can continue to <http://www.clinks.com>.

advisory provided by 

Figure 7. Warning page shown by Google

This page clearly warns that the site the user wants to visit may damage his or her computer. From the user's point of view, this is an interesting function, as it offers various options or advice: get information on how to protect their computer via the website of an antimalware organization of which Google is a member (StopBadware.org); return to the main search page and select another link; carry out another search with different keywords; or even access the potentially dangerous site.

What difference does this make for an average user faced with malicious websites? On the one hand, it offers a new level of protection against those websites which are widely recognized as malicious. Additionally, the fact that the site is not simply censored, but instead advice is given and options presented, (including that of visiting the site with the user assuming full responsibility), are positive steps in terms of educating users on the dangers of certain websites, all the while leaving them free to choose when it comes to browsing the Internet.



However, this approach has a disadvantage. Does the lack of a negative opinion mean that the site is trustworthy, or is it possible that it has not been cataloged yet? The fact that a group of dangerous sites are classified as such could lead the user to implicitly trust those sites which are not initially classified as dangerous. Of course, the identification of malicious sites is a positive move, and it does lead to increased user awareness – however, even at that it remains a double-edged sword.

Conclusions

Privileged positions are advantageous, but they are also exposed to increased attention from undesirable sectors.

It is an undeniable fact that Google is a “brand” that is recognized the world over. From this point of view, any effort made to improve information for its users will have maximum benefit. The fact that steps are being taken towards educating visitors to the site on malware and which pages are particularly malicious is much more than a symbolic gesture. It is a step forwards along a path to ensuring that those who browse the Net understand the dangers they are exposed to by carrying out even the most innocent of searches.

On the other hand, this very same privileged position means that Google, as well as all the other services and tools that make up the “brand”, represent one of the many areas of social engineering techniques that Trojans use in order to get users to voluntarily execute them. In this way, users are obliged to exercise caution and, as occurs in other areas such as phishing, they should not automatically trust those communications (email, etc.) which claim to originate from a specific company.



Orange Alert

A lot of water has flowed under the bridge since the last time Panda Software had to issue an alert. In fact, the last “shock” of this type was on December 23, 2005, with the appearance and distribution of the Banker.BSX bank Trojan, an event which caused the alert level to be raised to Orange.

Even further back was the first quarter of 2004, which represented an extremely difficult period of time: ten alerts (including six red) in less than four months.

However, during the month of September, it was necessary to dust down the bayonets and go back to the trenches.

Phishing/BarcPhish.HTML

On September 12 PandaLabs detected an increase in phishing activity, with the number of samples received surpassing normal levels by 30%. Once the samples were analyzed, it was seen that almost two out of every three messages were directed against the Barclays financial institution in the United Kingdom. This evidence pointed to a large-scale phishing attack on Barclays UK users.

The attack began with the receipt of an email that looked like this:

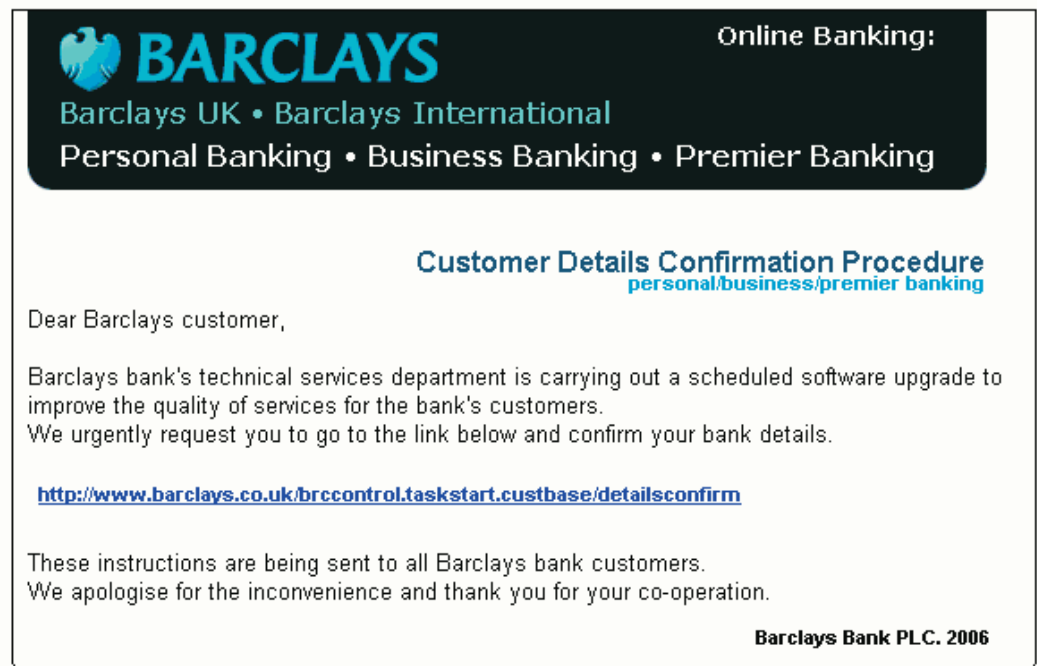


Figure 8. Content of the email that was sent

All the information that could be seen at first glance on the email suggested it was trustworthy: email address from the barclays.com domain, the company logo, corporate colors, etc.

However, it was all part of a cunning ploy: the link included in the email message was spoofed so that, when it was clicked, instead of going to www.barclays.co.uk, the user was re-directed to another site which imitated it:



The screenshot shows a website header with the Barclays logo. Below the header, there is a navigation menu with 'Details Confirmation' and 'Exit Page'. The main content area is titled 'Confirmation Procedure Step 1 of 2' and contains a 'Bank customer details confirmation page' with a warning icon and instructions: 'Please fill in all the fields on the form below. When you have finished entering the details, select the green "next" button to go to the next page.' Below this is a 'Your Details' section with a 'Please confirm your Barclays details' heading and a 'Help' button. The form is divided into several sections: 'Personal Banking' (with radio buttons for Personal, Business, and Premier Banking), 'Personal details' (with fields for Full name, Date of birth, MN, Home address, Home phone number, Work address, Work phone number, and E-mail), 'Bank card details' (with fields for Card number, Expiration date, and CVV), 'Online banking details' (with fields for Surname, Membership number (with '2010' next to it), Five-digit passcode, and Memorable word), and 'Phone banking details' (with fields for Account number, Sort code, Balance, Overdraft limit, and Phone banking passcode). At the bottom of the form is a green 'Next' button with a right-pointing arrow. On the right side of the page, there is a dark blue sidebar with the text 'Re-order your details online' and a 'Find out more' link with a right-pointing arrow.

Figure 9: website accessed when the spoofed link was clicked on

As can be seen in figure 9, a huge number of details were requested:

- Bank card details: card number, expiry date, CVV (Card Verification Value).
- Online banking details: Surname, membership number, 5-digit password, security password.



- Telephone banking details: Account number, branch identifier, balance, limit, password for telephone operations.

Logically, any information entered on the form would end up in the hands of the fraudsters behind the entire scheme.

As if this were not enough, an additional detail meant that this attack could easily go by unnoticed: once the details were entered onto the form, the web browser was redirected to the legitimate Barclays website, so as not to arouse any suspicion with the victim.

Finally, several days later the quantity of email messages began to decrease, and the orange alert returned to its normal status (green). This, however, was not to last too long.

Great number of active malware

As we have already mentioned on numerous occasions, the main aim of malware today is to achieve economic benefit through fraudulent means, using any methods available.

This is malware that has been designed to gain access to the access passwords for online banking institutions (through phishing or the registration of keystrokes, for example). It is a type of threat that is becoming increasingly difficult to eradicate, such as bot networks, groups of infected computers that are used in order to send spam or install adware. It is the existence of vulnerabilities which have not yet been documented, but are actively used to gain control of vulnerable computers.

Finally, it is also about what we could call malware “fragmentation”.

Look at a list of more-or-less well-known names: SQLSlammer, Mydoom, Bagle, Netsky, Sasser, Bugbear, Blaster, ILoveYou, Klez, Sobig. What do these families have in common? They are all worms, and at least one of their multiple variants created an orange or red alert situation **during 2004 or before**. They are all charismatic names, and are referred to when talking of the great mass epidemics.

How many can you think of that relate to mass epidemics from 2005? They are there, but are much fewer in number, with not-so-familiar names. As for 2006, those epidemics in which worms play the starring role can be taken as well and truly over.

However, this does not mean that active malware is any less widespread. Instead, the malware that is in circulation is being fragmented. There is no longer a single variant distributed to the four corners of the earth, but rather a huge number of variants which, individually, have very limited distribution but, when considered as a whole, they can become as notorious as the most famous worms of all time.

Nevertheless, on many occasions the language and forms of action of the antivirus industry has not changed when it comes to informing about current malware dynamics. For example, the Panda Software Global ThreatWatch, which offers updated information on the malware situation around the world, remained at Green level (normal), as there was no specific threat which merited the declaration of a state of alert. However, the existence of a permanent Green status gave a false feeling of security, which had nothing to do with the actual situation.

This can be seen in the following qualitative graph, representing the number of variants that have appeared in the different malware categories between 2002 and the current day:

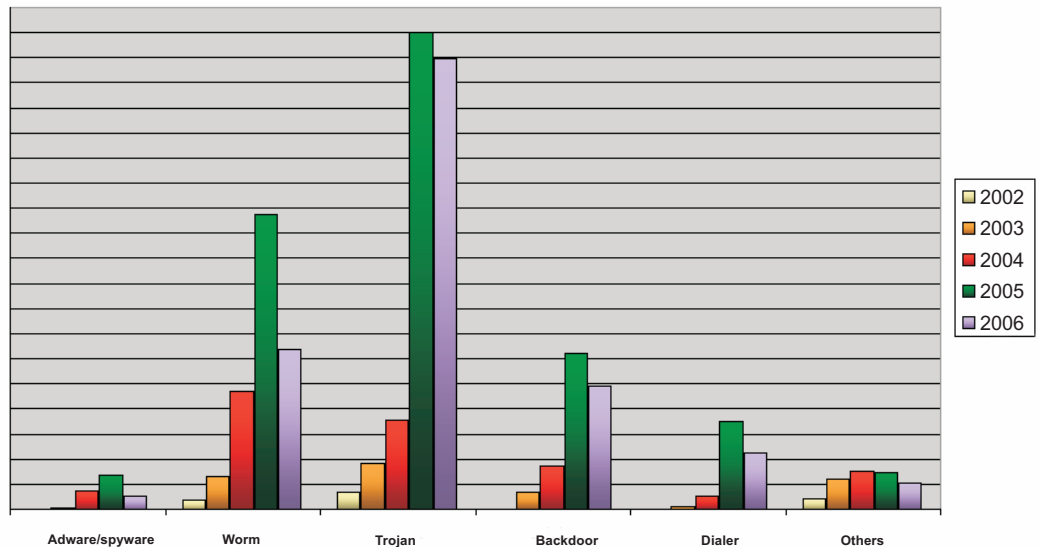


Figure 10. Variants of each malware category from 2002 to the present day

As we have mentioned, 2004 was the year of the great epidemics, accompanied by the subsequent media coverage this involves. Despite this, although 2005 easily surpassed this in terms of the number of appearances from malware types (covering almost every category), the number of alerts and their seriousness was not exactly higher. And although 2006 figures seem to be decreasing with respect to 2005, how many alerts have actually been declared so far in the year? When viewed in this way, we are still clearly above the levels of malware appearances for 2004.

To make this current malware dynamic more clear, we have decided to redefine the classification of alert levels, with the following results:

STATUS	DEFINITION
Green (Normal)	Normal situation. No mass-distributed specific threat. The malware in circulation remains within acceptable limits. Normal incidents. Low risk of being affected by a virus or malicious code, so long as normal precautions are being taken.
Orange (Pre-alert)	Pre-alert situation. There are one or more specific threats that are being spread on a mass basis, or the combined action of malware in circulation represents a serious risk. Significant incidents. High risk of being affected by a threat.
Red (Alert)	Red alert situation. There are one or more threats being circulated on a mass scale, or the actions being undertaken by malware in circulation is extremely serious. Generalized incidents on an international scale. Extremely high risk of being affected by a threat.

Table 5. Current Panda Software alert status classification

In this way, an alert situation can be declared based either on the mass propagation of a specific threat, or on the quantity of dangerous malware that is currently in circulation. Our Global ThreatWatch has modified its status, to warn users of the danger:



Figure 11. Global ThreatWatch displaying the current alert status.

Periodically, in addition to various statistics, Global ThreatWatch also displays the following descriptive phrases:

- Hundreds of banker Trojans and other threats designed to steal confidential data are silently infecting computers.
- At the moment there is a high risk of suffering an IT attack: make sure that your computer is correctly protected.
- Scan your computer with an updated antivirus as soon as possible.

Conclusions

Up until 2004, the declaration of an Orange or Red alert status showed the existence of a specific type of malware which was being massively distributed throughout the world. This was a very specific condition, and was produced on various occasions.

However, all of this was to change significantly in 2005, because the conditions that kick-started an alert were no longer checked, a situation which was stabilized during 2006.

Through the redefinition of the Alert Status and the establishment of an orange alert that was not associated to any specific type of malware, it is hoped that users will be made more aware of the current malware dynamic, and thus not let their guard down. Despite the fact that the mass epidemics of years gone by are no longer being registered, the situation has become worse, and malware is now more dangerous than ever.



Other news in short

America On Line publishes its users' searches

At the beginning of August America On Line decided to make public the text strings that 658,000 users had included in over 23 million searches over a three-month period.

In order for all this information to be analyzed by researchers, it was stored on a website.

Although America On Line stated that the published information contained no identifying code that could single out a particular user, this was proved to be false when the New York Times was able to identify at least one user based on the searches that he or she had carried out.

However, when the company decided to remove user data from the website, this had already been downloaded by users all over the world and stored on other websites.

Over and above the curiosity arising from looking at exactly what was being searched for, it is clear that the publication of these details could seriously damage the privacy of those users affected. Furthermore, more sensitive details may also be endangered, such as social security numbers, if they had been the subject of a search.

This was such a serious slip-up that the CTO (Chief technical Officer) resigned, and various employees were fired.

25th anniversary of the PC

On August 12 1981, IBM launched its IBM 5150 computer onto the market.

Despite the fact that the companies expectations were to sell 250,000 units over the following five years, they finally managed to sell a million in just four years.

IBM 5150 was the predecessor of the vast majority of modern computers, and still enjoys a good reputation, with 200 million units sold every year around the world.

CarderPlanet: malware professionals

"Looking for professional solution? Discover the power of technology. The most creative ideas. Professional researches. Precise and impartial approach. Individual customer support. Providing best solutions. The team you can rely on. Everything you need for business."

No, this isn't a script for a Panda Software commercial, although you could be forgiven for thinking so. It's a list of sentences that appeared on an advertisement for the CarderPlanet criminal group, through which they promoted their illegal activities.

The advertisement was used at the DefCon Conference in Las Vegas at the beginning of August, as an example of the levels of professionalism that are being reached by malware creators, even to the point where they are shooting videos to attract clients to their illegal business.



Spamta worms: first contact

On August 15 the first variant of the Spamta worm family was detected. This is a family which, throughout the rest of the quarter, was to increase to more than 130 variants, all launched simultaneously in waves of dozens of variants each time.

This family of worms, also known as WarezoV and Stration, spreads via email, disguising itself as an error message from the mail server.

Vulnerability in Vector Markup Language (VML)

On September 18 Adam Thomas, researcher with Sunbelt Software, discovered a website capable of executing code on a Windows computer that had all of the security patches that had been published up to that date.

The problem was due to a buffer overload in the VGX.DLL library, which renders VML (Vector Markup Language) graphics.

Versions 5.01 and 6 of Internet Explorer were critically affected, as was Outlook Express (as it uses Internet Explorer for certain tasks).

A few days later it was seen that a series of legitimate websites, hosted by the HostGator ISP, were being used to distribute malware through the exploitation of VML vulnerability. As was later discovered, HostGator servers had been affected through a vulnerability in the software used to control them.

In this way, we were facing a new zero-day, actively exploited before any security company or manufacturer had any knowledge of it.

Outside of the regular cycle, on September 26 Microsoft published the MS06-055 bulletin, which solved the problem.



About PandaLabs

PandaLabs is Panda Software'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 Software 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 Software 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.