QUARTERLY REPORT PandaLabs

(JULY - SEPTEMBER 2007)

PANDA SECURITY | *One step ahead.*

Content

Introduction

Once again we present the quarterly report which includes the most important IT security events in this quarter.

We have observed that malware creators have taken a rest, and that the number of malware samples detected has decreased over the summer. Even so, don't drop your guard, since the number of malware strains in circulation is still high.

The objectives of cyber-crooks however remain unchanged: to profit financially from stealing confidential information. This makes Trojans the predominant category of malware detected this quarter.

We have also observed a significant increase in the number of worms using IM programs to spread. Cyber-crooks take advantage of these programs' popularity used to exchange files, photos, music, etc.

As with previous reports, we will go over the most important vulnerabilities this quarter, and improvements in exploit methods. We will also mention the new vulnerabilities detected for which no patch has been released.

Kits using exploits to install malware are still an issue. In the previous report we offered you a global vision of these kits: general features, performance, etc. Due to the wide repercussion these applications have had among cyber-crooks, we have included a comparative review of the most popular kits, examining their main advantages and disadvantages.

And of course, we couldn't leave out our news and monthly logs sections, which includes a review of the most significant events of this quarter.

We hope you enjoy it.

The Quarter day by day

July 2007

Day 1:

Spanish National Police arrested a 24-year-old man from Barcelona who persuaded an underage girl from Alicante to pose nude in front of a webcam in return for a small amount of the profits obtained from distributing the images through online forums and chatrooms.

A California senator challenged a hacker to obtain the security codes to access the Capitol. The hacker managed to do so.

Day 2:

As the result of a scam involving the online sale of rural land for urban development, three companies in the UK were under investigation by the high courts for swindling over 250 people.

Day 3:

Tamara Broome, a 31-year-old Australian, tried to elope with a 17-year-old teenager she met during a game of World of Warcraft. She is facing charges for kidnapping a minor.

The Spanish Internauts Association alerted the police to a network of false web pages that purport to belong to (non-existent) Spanish financial entities.

Day 4:

The passwords for iPhone's root access were revealed in 3 days by analyzing the device's firmware.

AllOfMP3, a portal known worldwide and hosted in Russia which stored thousands of gigabytes of music was shut down by the Russian Government.

PandaLabs detected BotVoice.A, a Trojan which, when installed on computers, uses the Windows text reader to play the following sentences:
"You have been infected I repeat You have been infected and your system files have been deleted. Sorry. Have a Nice Day and bye bye".

Day 5:

The MPAA (Motion Picture Association of America) created a spoof website where users can supposedly download films with its own application. However, the page really aims to scan users' hard disks for pirate films.

IT experts conclude that security software, although costly, is worth its price.

The Quarter day by day

Day 6:

An old and still unpatched vulnerability in Microsoft Outlook can cause denial of service in Windows 2000 and XP Professional systems.

Hackers have started selling information about errors detected in different applications through a new online auction. This portal checks and validates the vulnerabilities before they are sold.

A Briton, a Moroccan and a Saudi Arabian related with Al Qaeda were accused of cyber-terrorism and could face six to ten years in prison for encouraging terrorism and the jihad over the Internet.

Day 7:

Spammers have discovered a way to automatically create Hotmail and Yahoo accounts and have bypassed Captcha's security measures to use accounts for spamming. Around 500 email accounts are created per hour. It is therefore very difficult to know how many of them are used for spamming.

Day 8:

Thieves are using stolen credit cards to make charitable donations. However, there is nothing philanthropic about this, as they are simply doing it to check whether the identification numbers are correct before selling them.

Day 9:

An unknown vulnerability in Yahoo! Messenger 8.1 was put on sale for 2,000 euros.

As a result of recent computer attacks against Estonia, the USA will study improvements to its own defenses and those of its allies.

A US federal court of appeal has estimated that federal agents do not need a search order to monitor suspicious users' computers.

The Pirate Bay, a site claiming to be the biggest BitTorrent tracker worldwide, could be added to anti-child pornography filter lists as a result of its deference to pedophiles and its defense of such delinquents' rights to 'freedom of speech'.

Supporters of The Pirate Bay appear to have launched an attack against the Swedish Police's website, polisen.se, causing it to be out of service due to continuous denial of service (DoS) attacks.

The Quarter day by day

Day 10:

Swedish Police will not include The Pirate Bay in anti-pornography filters since no real proof has been presented.

The new protection included in Blu-tray Disc BD+ films will make them impossible to crack for 10 years, since BD+ offers security features which have increased fourfold the barriers imposed by AACS (Advanced Access Content System).

Microsoft published six security bulletins (MS07-036 to MS07-041) as part of its cycle of releasing updates on the second Tuesday of every month. (3 Critical, 2 Important and 1 Moderate)

Day 11:

PandaLabs discovered a tool that controls a botnet with over 7,500 zombie computers infected by the Aifone.A bot Trojan. This tool can redirect users to a page similar to iPhone's official web page to obtain confidential data.

Day 12:

A new security hole affecting the 'firefoxurl://' function in Firefox browsers was uncovered. It allows intruders to install executable commands on the vulnerable system.

The US Secret Service has arrested four members of a criminal band responsible for the loss of 75 million dollars through trafficking 200,000 falsified credit cards.

The 25th anniversary of the first computer virus. The Morris Worm (1988) was the first malware sample with extensive repercussions. Elk Cloner did not seek to damage systems or data, only to annoy users a little by displaying a poem on the computer screen every 50 startups.

Day 13:

The Internauts Association is monitoring how the different security channels (national and European) act and how long they take when dealing with accusations that affect thousands of users. This is because since July 6, a spoof European Union job offer has been distributed massively via email.

Day 14:

The latest cyber squatting cases have targeted Spanish tourism. Attacks on travel agencies' websites have increased. These attacks consist of redirecting thousands of tourists who regularly visit the online agencies to book their trips, to other sites with similar offers.
Cyber squatting consists in registering domain names similar to those of the official websites.

The Quarter day by day

Day 15:
In an anti-child pornography operation, National Police seized 48 million online images and videos, and arrested and charged 66 people.

Day 18:
An independent hacker has developed a worm that exploits an unknown vulnerability in MAC OS X.
The worm can obtain superuser privileges by exploiting a variant of the mDNSResponder vulnerabilities that Apple resolved some time ago.

Day 19:
The Xbox console has been hacked, allowing users to play all videogames on 360, unlike up until now, when it was limited by regional format (PAL or NTSC).

Spammers have improved their techniques to bypass anti-spam filters. They now use PDFs instead of images.

Day 20:
Due to early sales of the final Harry Potter book in an online store, newspapers including the New York Times have confirmed that the digital version of the book is available on P2P networks.

Day 21:
In an interview with ComputerWorld Australia, Ed, a retired spammer, explained the sinister techniques used in the world of spamming, from which he managed to make a considerable fortune by sending promotional emails of pills, porn and casinos.
He said to have earned between $10,000 and $15,000 a week and $480,000 in his last year.

Day 22:
Microsoft revealed information about Windows 7 (previously known as Vienna) in a sales channel conference in Orlando. The launch plan for Windows 7 will adhere far more to the schedule and it could be ready in three years.
As with Windows Vista, there will be a consumer version and a version for professionals, as well as 32 and 64-bit versions.

The Quarter day by day

Day 23:

Four members of a gang kidnapped one of the best RPG (Role Player Game) players worldwide, who was then tortured for five hours to reveal game passwords, which could then be sold for $8,000.

A month after the Darketernal web portal was shut down and its administrator (creator of the infamous DVD 'Todo en Uno' – 'All in one') was charged, National Police agents have arrested 16 people accused of intellectual property crimes.

Day 24:

A vulnerability was confirmed in Wii. The exploit completely blocks Wii and runs through YouTube's .FLV format.

ISE (Independent Security Evaluators) tested a code which allows piracy and taking control of the iPhone when connected via WiFi to a page containing that code.
Once the device is controlled; the owner's contact address book can be copied, calls can be programmed or it can be disabled.

Day 25:

Denis Kvasov, creator of 'AllofMP3', a website where music is sold and swapped online, could face 3 years in prison due to serious copyright violation.
The district attorney also demanded that the accused paid a 15-million-ruble fine (427,000 euros) in damages to the music industry: EMI, Warner and Universal among others.

The independent Swedish distributor 'Labrador Records' offered internauts 68 MP3 track downloads for free, but its servers could not manage the workload. The most original solution was to access the popular BitTorrent tracker, The Pirate Bay, and distribute musical content without saturating its servers.

Day 26:

Several security experts have discovered a zero-day vulnerability in the *Uniform Resource Identifiers* of Firefox which affects the version for Windows, and allows hackers to control and gain complete remote access to the PC through a specially-crafted website.

The Quarter day by day

Day 27:

Due to the Anti-piracy Federation's (FAP) accusation against the "www.todotorrente.com" website, three web-page administrators have been arrested. The web pages provided downloads of movies on their release date, returning profits of over €30,000 and causing damage to rights owners valued at € 535,000.

Day 28:

Russell Tavares from Virginia (USA) drove to Texas to burn the caravan of a man he had argued with over the Internet.

The Catalan Police and the Spanish Civil Guard carried out an operation against online child pornography. A 41-year-old man from Oviedo and a 21-year-old man from Valencia have been charged with corruption of minors, and possession and distribution of child pornography.
They are accused of obtaining pornography in chatrooms by using the 'grooming' method, which consists in deceiving victims, pretending to be children and asking them for photos.

Spammers have started to use spreadsheets and ZIP files to distribute their 'advertising' massively.

Day 30:

A group of hackers known as 'S4udi-S3curity-T3rror' launched several intrusions and managed to enter dozens of websites of the Philippine government using zero-day vulnerabilities.
Philippine authorities have started to update their systems to eliminate the vulnerabilities.

Day 31:

Microsoft is planning to present a third Service Pack for Windows XP, which would further extend the useful lifespan of this operating system.
In August, 2004, Microsoft released SP2 and it seems like SP3 will be released in the first half of 2008.

An Australian user has managed to partially release the iPhone and make calls through another operator instead of meeting the condition of using AT&T. Nevertheless, a way in which calls can be received is yet to be discovered.

The Quarter day by day

August 2007

Day 1:

A study by ComScore revealed a significant increase in the number of online games users (now 217 million). This increase is proportional to attacks on online game servers, such as the ones that have taken place this year against Second Life, World of Warcraft, Lineage, etc.

Internet rumors claim Microsoft is preparing the release of 2 security patches that will make up Window Vista's first Service Pack (SP1). As usual, Microsoft will release these patches on the second Tuesday of August.

The New Yorker magazine claimed that 'spam' began in the spring of 1978, when Gary Thuerk wanted to publicize the launch of his new company. To do so, he sent an email to thousands of Arpanet network users, causing the first 'spam attack'.

Day 2:

Second Life banned casinos due to legal conflicts in several countries. The measure will not only disappoint users, but also the companies who have invested in virtual advertising through casinos.
US federal agents searched over 30 stores and homes looking for Wii and PlayStation 3s adapted to play pirate videogames. It is thought that modified chips and devices have been distributed in 16 US states.

Day 3:

Polish security specialist Joanna Rutkowska once again used her infamous Blue Pill, a malware strain that enters Vista's virtualization system and grants supervisor privileges, to demonstrate that the vulnerability hasn't been resolved as Microsoft previously claimed.

Attacks on banks worldwide have increased by 81 percent in the last year, according to data revealed on August 3, in the Black Hat security conference.

Day 4:

Microsoft has been forced to drop the price of Windows Vista in China due to the high number of pirate copies distributed. Use of pirate software versions in China is estimated at 80 or 90 percent.

The Quarter day by day

Day 6:

The blogger who passed himself off as Steve Jobs was uncovered. The mysterious author of The Secret Diary of Steve Jobs was really Daniel Lyons, editor of Forbes magazine, who is now preparing to launch a novel about his activities during the fourteen months that he remained incognito.

A new phishing scam involved the sending of thousands of emails claiming to come from the tax authorities. The emails tried to trick users into revealing confidential data such as, credit card passwords, by offering details of tax rebates.

Day 7:

The latest experiment by the Chinese government to cure youngsters of their Internet addiction is to create a summer camp for 40 youngsters (14-22 years old) identified by psychologists as 'cyber-dependent'. For ten days they will be treated for; depression, fear, inability to interact with others, panic attacks and restlessness.

Day 8:

At the Black Hat event, one the most important events in the IT security calendar, a security expert surprised everyone by carrying out a live demonstration of how to hack a Gmail account, proving the feasibility of what web-based email providers go to great lengths to deny.

Day 9:

The code of the latest version of the popular P2P BitTorrent software will not be distributed in open-source code to developers. The software will continue to be free, but its code will not be accessible as before.

Day 10:

The British government is evaluating the possibility of increasing budgets, improving the training of IT security police and establishing a centralized system to monitor cyber-crime such as, measures to protect citizens from online fraud.

Day 11:

The Australian government has reported it will invest 162 million dollars in Netalert, a program aimed among others, at shutting down cyber-terrorists' sites and reducing the pornography accessible to Australians.

Day 13:

Hackers have bypassed the protection of the UN website and have displayed a message protesting against Israeli and American politics. A few hours later, the UN blocked access to the affected web pages and published a message apologizing for the inconvenience caused.

The Quarter day by day

Day 14:
According to IT experts, Microsoft has launched the most important package distributed this year. This package contains nine patches that solve 14 security flaws, six classed as 'critical'.

Day 16:
Ubuntu shut down five out of eight servers last week, when it discovered they were being used to attack other systems. These servers run with an old and outdated version of Ubuntu, which could explain to some extent why they became unsafe.

Day 17:
Skype's online telephony service was out of use during most of the previous day. Consequently, its 220 million users were unable to carry out phone calls. This was due to an error in all Skype copies downloaded since 2003.

Chinese cyber-dissident, Chen Suging, who posted articles against communist authorities on the Internet, was sentenced to four years in prison for "inciting the government's overthrow". Reporters without borders have reported it.

Day 18:
Australian authorities have arrested the hacker who recorded the 'The Simpsons' movie with a cell phone. Before being arrested, he published it on the Internet, where it was downloaded 110,000 times before being withdrawn.

PandaLabs detected MSNHorn.A, a worm that downloads numerous samples of malware onto affected computers and spreads through MSN Messenger.

Day 19:
The 25th anniversary of the CD. Happy birthday!

Day 20:
PandaLabs detected Nugache.M, a Trojan that can obtain users' confidential information such as passwords, by recording users' keystrokes. It also disables the Windows XP firewall and connects to an IRC server to receive instructions (i.e. carry out denial of service attacks).

The Quarter day by day

Day 21:

A study by a technology consultant indicated that in the professional sector, email has replaced the telephone as a means of communication. Some 99.6% of the 524 companies studied (13 countries), used email to communicate with other company members.

A Trojan attack could have allowed hackers to access personal information of hundreds of thousands of users of the popular Monster job portal. This information was used to send users customized phishing emails.

Day 24:

A hacker was convicted of loading the movie Star Wars: Episode III on the Internet to be shared with other users, and has been charged with criminal copyright violation. After spending 5 months in prison, he was forced to install a monitoring tool on his computer. But since he used Linux, and the tool was not Linux-compatible, he will now have to use Windows when using the PC.

It is now 25 years since Windows 95 was launched. This solution set a milestone in Microsoft's global history.

Day 26:

16-year-old Australian, Tom Word, managed to disable a multi-million dollar, government anti-porn filter. It took him around 30 minutes to disable the 84-million-dollar filter.

Day 28:

A rootkit was discovered which installs itself on the PC while using Sony's USM-F flash memory with fingerprint reader software. The rootkit's aim is to hide in a folder that can be used for malicious purposes.

Day 29:

China created a virtual police patrol which will display a cartoon pop-up on internauts' computers every 30 minutes to remind them their online activities are being monitored.

Day 30:

After three months' speculation, Microsoft provided the specifications of the Service Packs for its operating systems (Vista and XP). The installation of Windows Vista SP1 will require 7 Gigabytes of free disk space for x32 machines, and 12 Gigabytes for x64, although most of the space will be freed up after installation.

The Quarter day by day

September 2007

Day 1:
Hackers used the website of a bank in India to infect PCs with banker Trojans. Several IFRAMES were injected on the page to detect system vulnerabilities and exploit them to introduce malware on users' PCs.

An online pyramid sales scam was discovered in China. Investors paid 8,000 yuans each (less than one euro) and were told they would receive 400,000 (nearly 38 euros) within 30 months. 170,000 people are said to be involved and the amount swindled is estimated at 132 million euros.

Day 2:
German secret services are evaluating whether to create Trojans to install on suspect computers. This measure has been taken because of spyware –allegedly from China- detected in May on computers belonging to the Chancellor and several other ministries.

A denial of service vulnerability was found in the strategy game StarCraft, causing the system to block. To exploit it, users would have to download a specially-crafted map.

Day 3:
PandaLabs detected Kimo.A, a worm that modifies the Windows Registry to prevent the computer from working correctly. It then restarts the computer.

Day 4:
In June, a group of Chinese soldiers attacked the Pentagon network. Investigation continues, although it appears that the stolen information is unclassified. This attack places China in the spotlight again after the attacks detected in May by German secret services.

Day 5:
A man from Illinois was sentenced to 30 months in prison for distributing pirate software. He was accused of distributing 20,000 pirate copies of video games, films and music illegally, including pre-release versions.

Day 6:
PandaLabs detected Gnome.D, a virus with worm characteristics, aimed primarily at spreading and infecting as many computers as possible. It spreads by infecting PE files, through email and the mIRC program.

The Quarter day by day

Day 7:
Downloading music or movies on the Internet as long as it is non-profit making is not a crime in Spain. Consequently, Promusicae, the association of music producers, is unable to take any action against Telefonica, who refused to reveal personal data of users who downloaded files on the Internet.

Day 9:
In addition to Germany and the USA, France has also fallen victim to Trojan attacks that allegedly originate in China. China continues to deny these attacks.

The FBI will not be able to spy on users over the Internet or the phone. This is what a judge has decided six years after the US Patriot Act, allowing the FBI to do so, became law.

Incredible as it may seem, Comcast has removed Internet connections from several American users due to excessive bandwidth use. According to Comcast, this affects other users' bandwidth capacity.

Day 10:
PandaLabs detected the FakeGoogleBar.M and Lunchload.A Trojans.
FakeGoogleBar.M collects information about users' browsing habits, such as the words entered on browsers when carrying out searches.
As for Lunchload.A, it connects to a specific server from which it receives instructions (e.g. to download and run new malware).

Day 11:
P2P file-sharing through BitTorrent faces a new enemy: porn producers. This tracker is causing losses to the porn industry of up to $2,000 million.

The government of India would like to install keylogger-type programs in cyber-cafes in Mumbai (formerly Bombay). This measure is aimed at detecting possible terrorists who could use these connections.

Day 12:
A shop that sold a client a laptop refused to repair it claiming the client had installed Linux. Although the laptop had a manufacturing defect, the shop considers the client's replacement of Windows Vista with Linux a "warranty violation".

The Quarter day by day

Day 14:
A Chinese student sued Microsoft for obtaining personal and private information after he installed Windows Genuine Advantage. He is also asking Microsoft to pay a $180 fine and a issue public apology in a national newspaper.

Day 16:
EADS, the large European aerospace corporation has developed an encryption system said to be 'hacker-proof'.

A 700-megabyte file was leaked in MediaDefender's (anti-piracy company) internal mail. The file, which can be downloaded from BitTorrent, uncovered dubious strategies the company uses to combat P2P networks.

Day 17:
A 30-year-old Chinese man died from a heart condition after a three-day Internet gaming binge. Increasing Internet addiction has seen the Chinese government take several measures, such as creating summer camps for young 'cyber-dependents'.

It has now been 16 years since Linus Torvalds invented Linux. Unlike other operating systems, its source code is publicly available so anyone can use, study and even modify it.

The Luxembourg court has rejected Microsoft's appeal, and it will therefore have to pay a €497 million antitrust fine. In 2004, the European Commission asked Microsoft to provide competitors with information so they could manufacture Windows-compatible products. Microsoft refused to do so.

Day 18:
On September 18, 1982, Scott E. Fahlman, computer scientist at Carnegie University (Pittsburgh), created the smiley ':-)', the first and most famous emoticon in history. Happy birthday!

Day 20:
PandaLabs detected Sohanat.DB, a worm that blocks access to several search engines, redirecting users to a web page similar to Google's which contains malicious links.

The Quarter day by day

Day 21:

According to a report by the research company ChangeWave Allliance, companies are not in a hurry to adopt Windows Vista and prefer to install XP. This could be due to the fact that its current users are not totally satisfied with this operating system.

The Internet observatory has detected at least fifty web pages which offer false qualifications and studies in non-existent higher education centers. These scams are usually advertised through spam, where users can get a diploma for 250 euros.

Day 22:

In view of the attacks reported by the USA, Germany and France which seem to come from Chinese hackers, Beijing has published a military report claiming China has also fallen victim to cyber attacks.

Day 23:

The famous tracker, The Pirate Bay, criticized several record companies and producers days after the information about the malicious techniques used by MediaDefender against piracy was leaked. MediaDefender collaborates with the most important record companies and producers in their fight against piracy in P2P networks.

Day 24:

The creators of Radoppan (Fujacks) whose symbol is a panda burning incense, were arrested. This virus caused serious problems in China, infecting thousands of PCs.

Day 25:

Madrid police have arrested four people for recording movies in cinemas, a crime that is on the increase. Several recorders, copies of movies and IT material have been seized in 'Operation Caviar'.

The beta version of Windows Vista Service Pack 1 was published, although it is only accessible to a small group of people. The service pack is aimed at solving several irregularities found in the new operating system.

An error has been detected in Excel 2007; a multiplication error occurs when the result of the formula is 65,535. Microsoft hasn't yet come up with a solution.

The Quarter day by day

Day 26:

It seems as though luck is on the side of Li Jun, creator of one of the most dangerous viruses in China. Although he was recently sentenced to four years in prison, a Chinese communications company has offered him the position of Technology Director, with earnings of €140,000 a year.

It may not seem like it, but dictionaries are no longer out-of-step with new technologies. From now on, words such as, adsl, blog and sms can be found in Spanish dictionaries.

A remote code vulnerability was found in OpenOffice. The vulnerability affects graphic files with TIFF compression and causes buffer overflows.

Day 27:

Since today is Google's 9th anniversary, it displayed a large pinata-shaped 9 on its website, as it does on special occasions.

Microsoft found an explanation for the mysterious error in the Excel formulas and is currently developing the corresponding patch.

Day 28:

The hacker Petko Petkov has discovered a serious security flaw in Gmail. First, a web page is created, which when visited and while internauts are registered in Gmail, installs a malicious filter in users' accounts to access their mail. Google is already working on a solution.

Day 29:

PandaLabs detected Ganensar.A, a worm that makes several modifications in the Windows Registry affecting computer operativity. It can also modify Windows protected files, which could cause problems in the operating system.

The Quarter day by day

Highlight news

Unhappy ending

Tamara Broome, a 31-year-old student from Adelaide University (Australia), could face 2 up to years in a US prison charged with trying to kidnap a 17-year-old boy from Greenville (North Carolina). She is said to have begun an intense relationship with the boy a year ago, through the online game World of Warcraft.

Broome flew from Australia to New York to take the youngster to Australia.

On June 12, the boy's parents reported his disappearance. A few days later, the police found the couple in the Raleigh-Durham International Airport (North Carolina) trying to fly to Australia.

Broome has been in prison, in the Pitt County Detention Centre (North Carolina), since June 26 awaiting the magistrate's decision.

Man attempts murder after online 'nerd' snipe

A man drove 1,300 miles (around 2,000 kilometers) from Virginia to Texas to burn the trailer of a man he had argued with on the Internet.

27-year-old soldier Russell Tavares saw red when Anderson (59) called him a 'nerd' online. Anderson posted a digitally altered photo of Russell under a "Revenge of the Nerds" sign. Russell got into his car and started driving. As he made his way toward Texas, he posted photos online showing the welcome signs at several states' borders, as if to prove to his Internet friends that he meant business.

When he finally arrived, Tavares burned his 'enemy's' trailer down. Anderson barely escaped.

Tavares was sentenced to seven year in prison.

After Tavares was arrested, John G. Anderson said: "I didn't think anybody was stupid enough to try to kill anybody over an Internet fight".

The Quarter day by day

Highlight news

RPG player kidnapped for password

Four members of a gang kidnapped one of the world's top RPG (Role Player Game) gamers, and tortured him for five hours to get his passwords and sell them for $8,000.

They used one of their member's girlfriends to entice the player, who is apparently a world leader in the game Gun Bound.

He turned up at a shopping centre in San Paulo for a date with the girl, but the gang was lying in wait and kidnapped him.

He resisted torture for five hours, claiming he would rather risk death than hand over his passwords. In the end they let him go.

Brazilian police caught the four suspects, aged 19 to 27.

Thousands of records stolen from Monster.com

Cyber-crooks used a Trojan -detected by Panda as Trj/Sinowal.FY- to steal confidential information from users of the famous job portal.

The site's representatives have admitted that hackers have stolen more than 1.6 million records.

Since users' records did not include bank details, hackers were after email addresses and personal information which could be used for customized phishing attacks. This way, they tried to fool clients to obtain bank account and credit card details. Users could have received an email with Monster's corporate image including job offers that coincide with their profiles, to fool them and obtain the information to carry out the scam.

The email could contain two files, which when run, install two dangerous programs: the *keylogger* records the passwords users use to access bank accounts; and the *ransomware* encrypts several computer files demanding a ransom for its restoration.

Monster has told its users that its website will never ask for their bank details.

The Quarter day by day

Highlight news

Spam is served

'The New Yorker' published an interesting article about the way spam came about.

It claims that spam is older than people think. In the spring of 1978, Gary Thuerk, who worked in the marketing department of DEC, wanted to publicize the launch of his new company, and came up with an ingenious idea.

His idea consisted of using ARPANet (The Advanced Research Projects Agency Network) which had thousands of users. He selected several users who lived in a specific zone he wanted to target and sent them an email with the following message "We invite you to come see the 2020 and hear about the DECSystem-20 family".

The results were excellent, and DEC sold 20 of its machines for a million dollars each.

Gary Thuerk became the founder of spam.

Smiley's 25th birthday

On September 18, 1982, Scott E. Fahlman, research fellow at Carnegie University (Pittsburgh) created the smiley ':-)', the first and most famous emoticon in history.

He came up with the idea after someone sent an email joking about contamination in an elevator, which created a debate about the limits of online humor.

Consequently, Fahlman sent the following message: "I propose that the following character sequence for joke markers: :-)", he wrote. "Read it sideways," he suggested.

Fahlman's suggestion was well received among students and employees at Carnegie Mellon University and the smiley expanded quickly to other universities and forums through the then rudimentary Net.

The message was loaded onto the e-bulletin on September 19, 1982 at 11:44. However, Fahlman never imagined the repercussion his creation would have and didn't save a copy of the message.

For years, the original emoticon was lost, until a University co-worker, Jeff Baird, and three friends found it and made a heroic effort just in time to celebrate its 20th anniversary.
The original message read:

The Quarter day by day

Highlight news

```
19-Sep-82 11:44    Scott E  Fahlman             :-)
From: Scott E  Fahlman <Fahlman at Cmu-20c>

I propose that the following character sequence for joke
markers:

:-)

Read it sideways.  Actually, it is probably more economical to
mark
things that are NOT jokes, given current trends.  For this, use

:-(
```

This icon has revolutionized cyber-space non-verbal communication: the small smiley has managed to bypass the limits of written communication which is unable to express emotions or facial expressions.

With the use of a colon, a dash and a bracket, smiley has no doubt avoided a few arguments among internet users.

Third quarterly figures

Distribution of the new threats detected

The graph below illustrates the distribution of new variants by type of malware detected by PandaLabs in the third quarter of 2007:

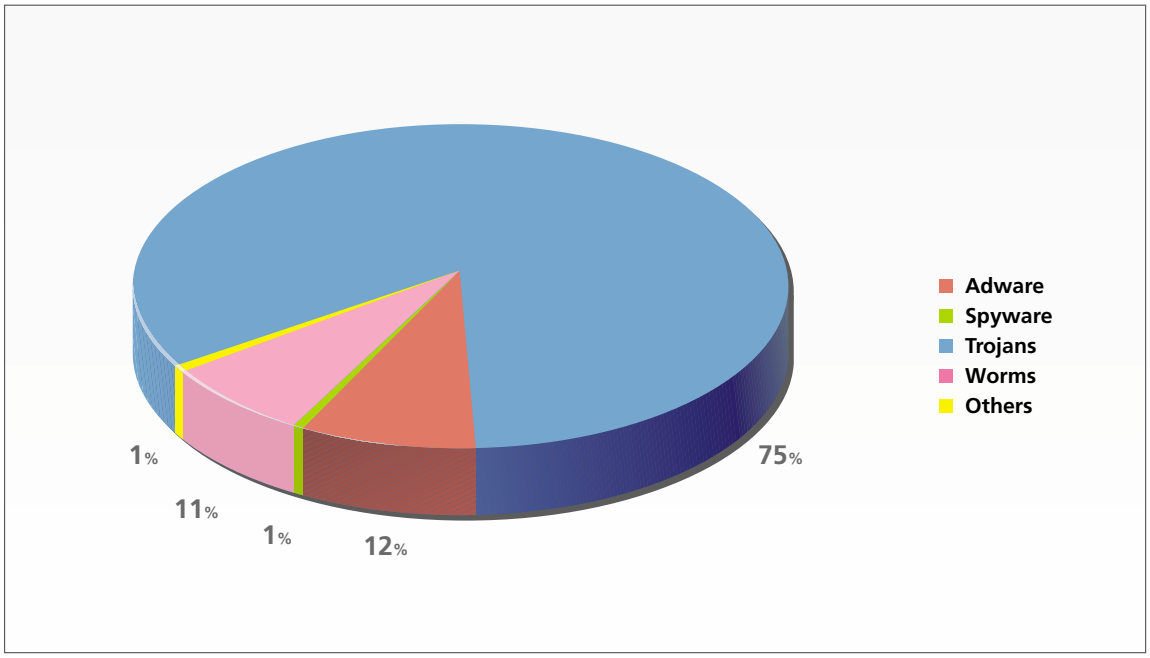


Figure 1. New malware variants detected by PandaLabs

Trojans were clearly the most prevalent type of malware in Q3, even though they decreased by 10% with respect to Q2 (84%).

Worms increased by 3%, confirming that malware creators are still endeavoring to spread malware as rapidly as possible, especially through instant messaging clients.

The sub-category of Backdoor Trojans has been included in Trojans. Bots have been included in the categories of worms or Trojans depending on their specific nature.

Whereas the amount of Adware and Spyware in Q2 was 7% of the total, this figure increased to 13% in Q3.

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

Third quarterly figures

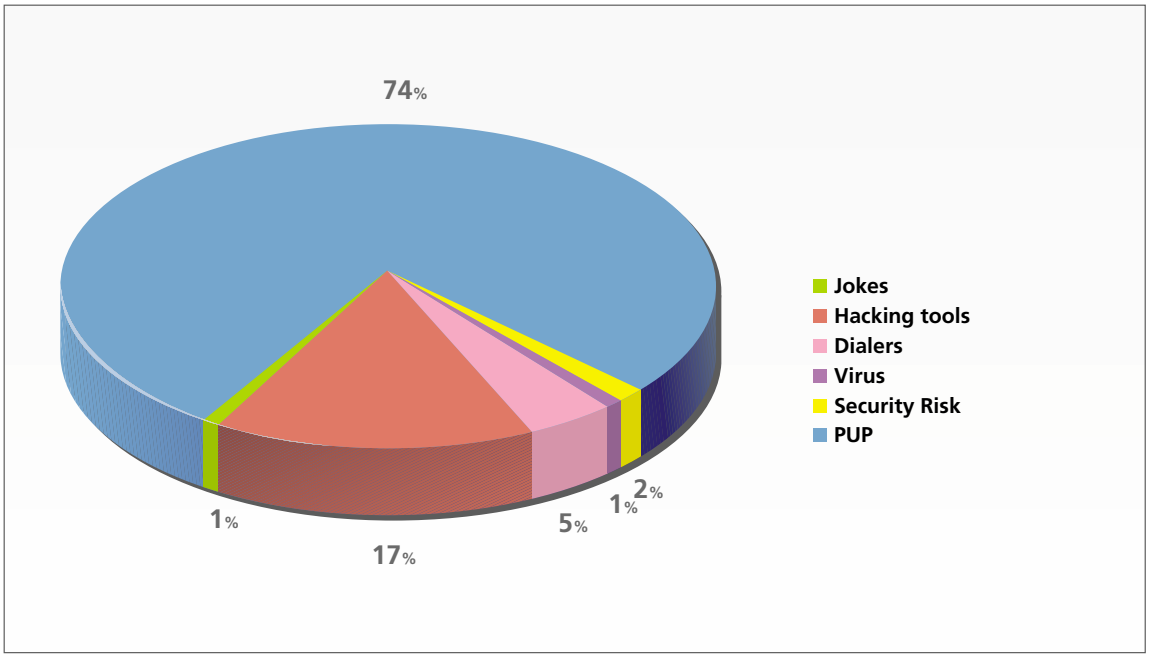


Figure 2. Classification of the 'Other' category

Within this category, PUPs (potentially unwanted programs) have increased by 26% compared with Q2.

The significant decrease in viruses (from 5% in Q2 to 1% in Q3) is due to the fact that malware creators are more interested in financial benefit than simply destroying systems.

The increase in the number of users with broadband connections has seen dialers drop considerably to 14%.

Third quarterly figures

Month by month

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

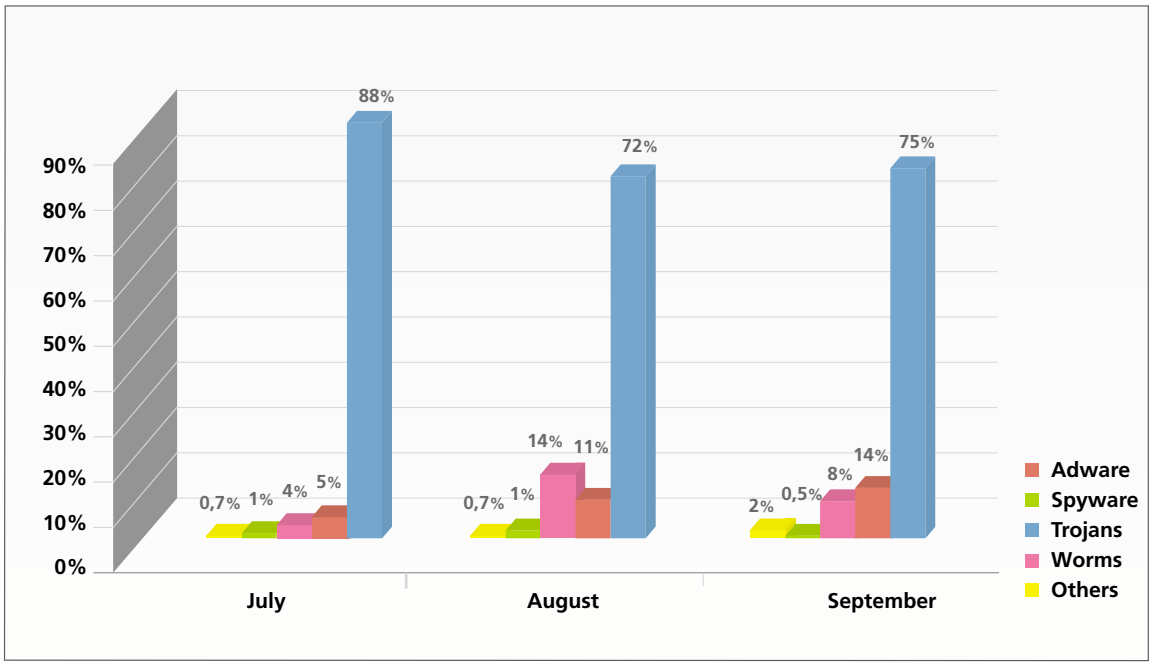


Figure 3. Appearance of new malware month by month

Third quarterly figures

Threats detected by Panda ActiveScan

The following graph shows the distribution of detections made by the Panda ActiveScan online scanner throughout the third quarter of 2007.

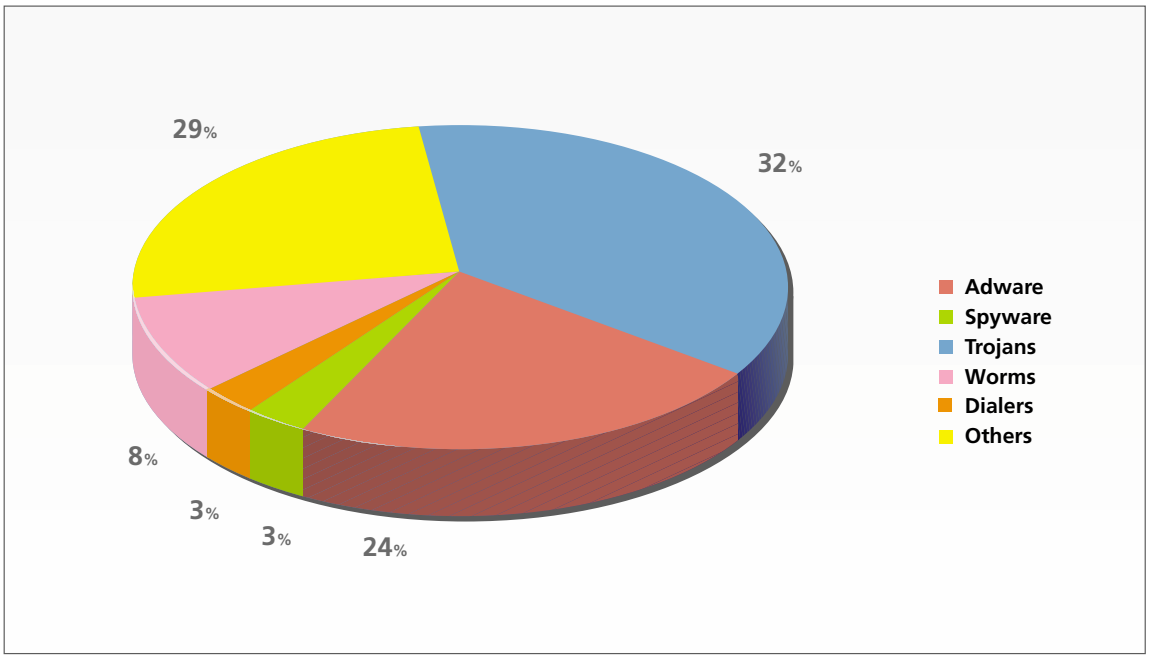


Figure 4. Detections carried out by Panda ActiveScan

With an infection ratio similar to last month's, Trojans continue to be the most active malicious code, detected on 32% of computers scanned.

Dialers continue to fade quarter by quarter (from 4% in Q2, to 3% in Q3).

Adware and spyware together stay at approximately 27%.

Comparative review of kits for installing malware through exploits

Here we take a look at the most active "kits for installing malware through exploits" on servers that are infecting users with malware.

IcePack

This is the most feature-rich kit, although it has one major disadvantage: the language (Russian). We have recently found an English version on the Internet, but we don't know if the translation has been carried out by the kit creators –the IDT Group- or someone else.

In these cases, it is quite common for users of these programs or visitors to forums with these types of tools to make improvements to the tools, modify them and even share and exchange them with other users.

This kit is the only one that has its own iframer:

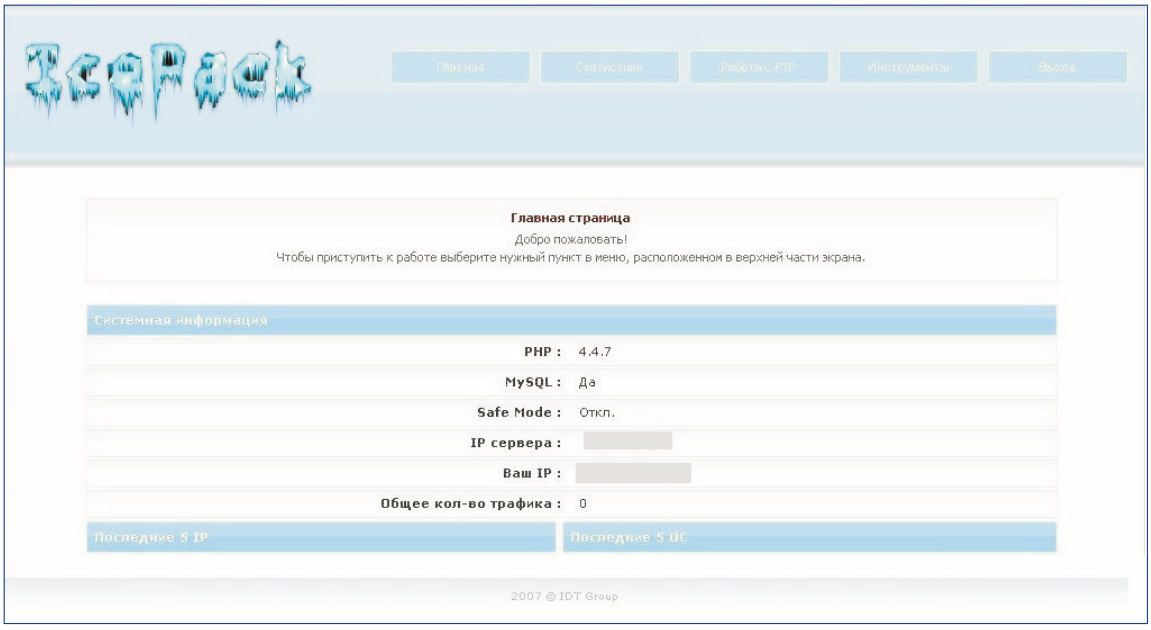


Figure 5. Control panel of l IcePack

In July this year we published a post on the PandaLabs blog with more information about this kit.

Comparative review of kits for installing malware through exploits

Mpack

This is a good alternative to IcePack, as both are quite similar. The only drawback is that it doesn't have its own iframer. This means that users would have to use an external iframer together with this kit to maximize the number of infections on web pages.

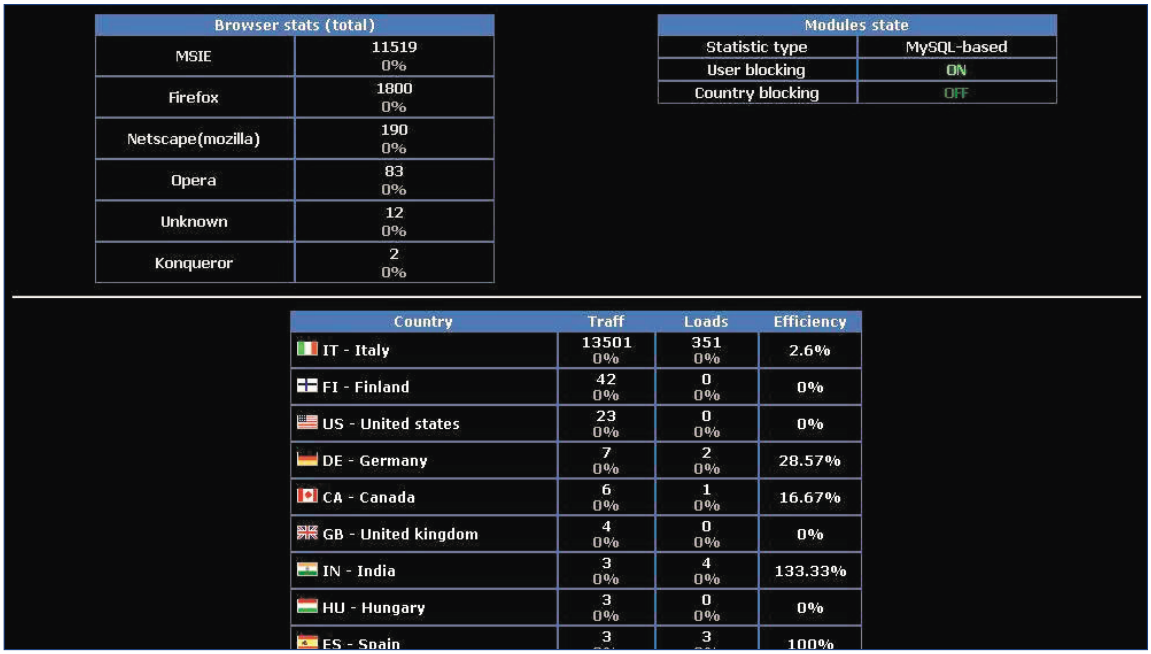


Figure 6. Control panel of Mpack.

You can check out the report we published about this kit last May on the PandaLabs blog.

Comparative review of kits for installing malware through exploits

Traffic Pro

This kit doesn't include exploits, so you have to add them before using it.

Besides, like Mpack, it doesn't have its own iframer.

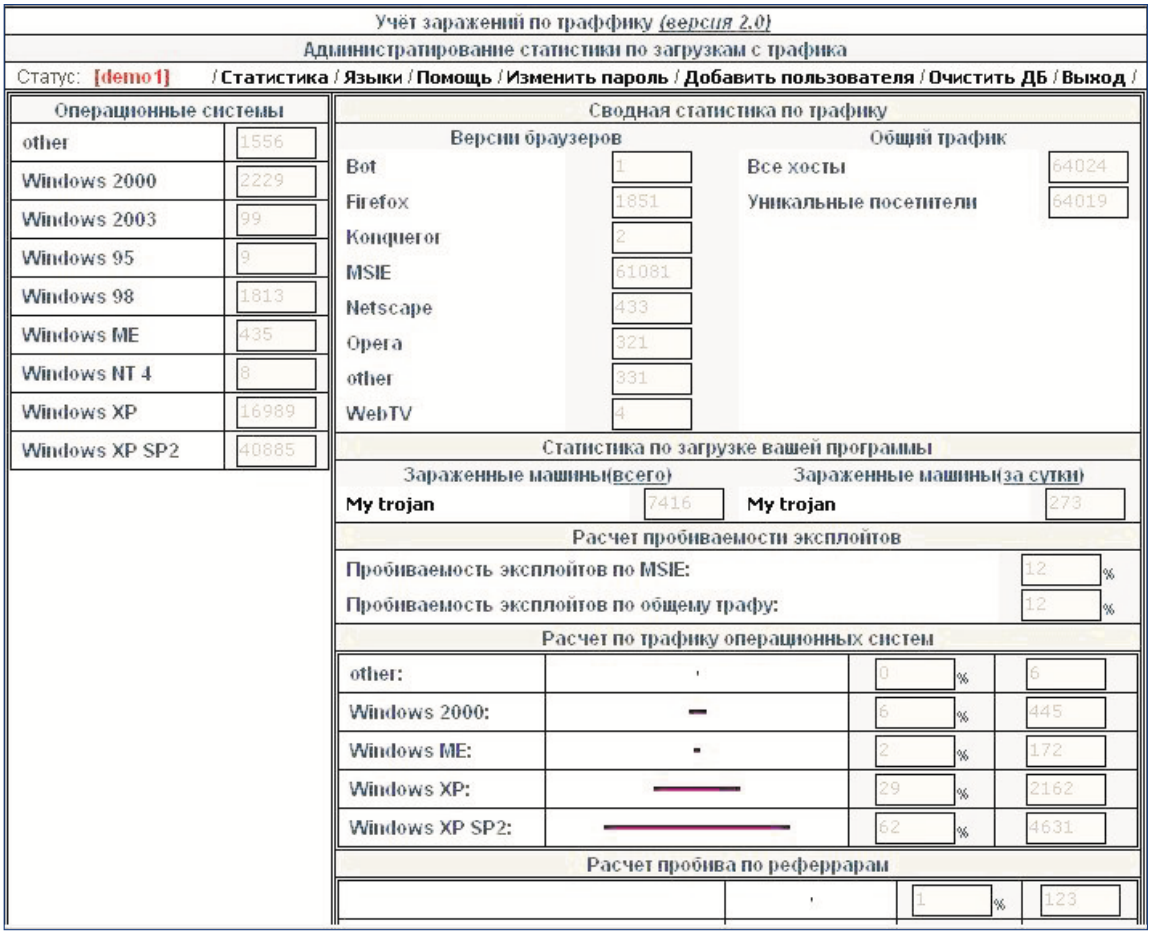


Figure 7. Panel de control del Trafic Pro

You can check out our report about this kit on the PandaLabs blog.

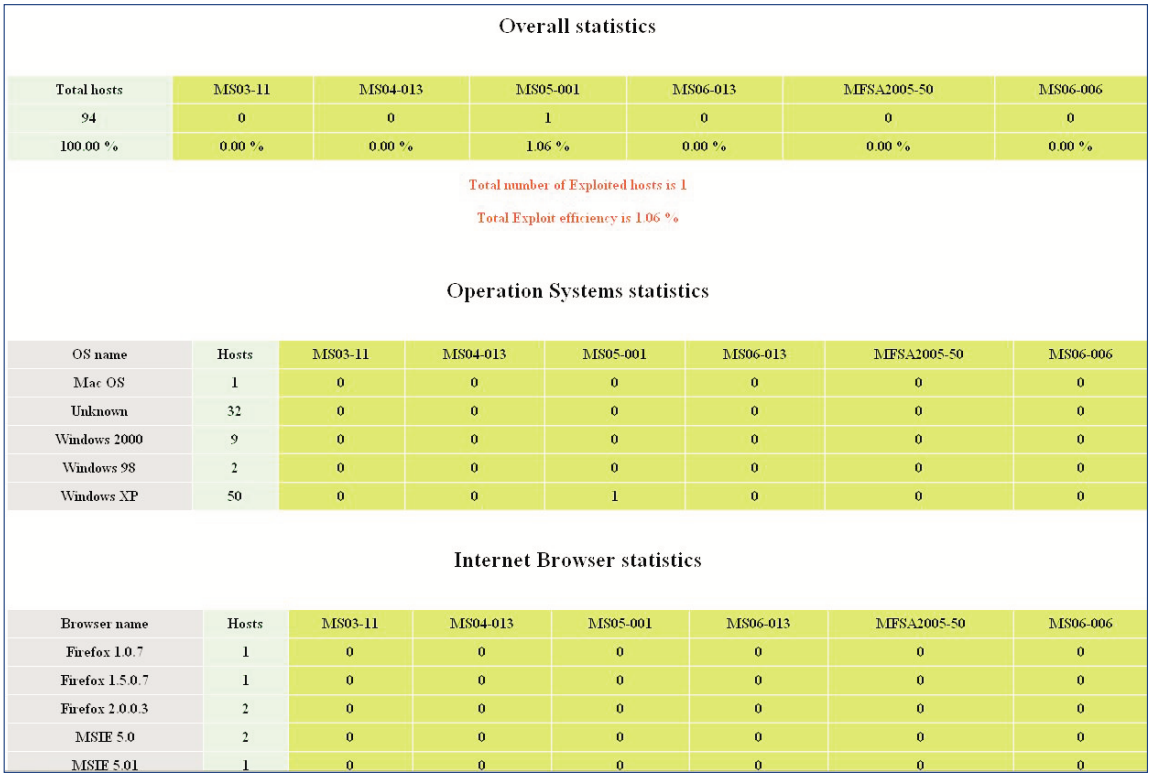
Comparative review of kits for installing malware through exploits

Web-Attacker

Of all the kits in this review, this one has the least features. Besides having the same disadvantages as the previous ones, it is programmed in Cgi instead of Php +MySql, making it even less compatible with certain servers.

This kit uses outdated exploits, and is therefore less effective when it comes to infecting users. Due to its design, adding new exploits manually is even more complex than with "Traffic pro".

Mpack creators recently said that they know the Web-Attacker creators and they are working on a new 2.0 version soon to be released.



Overall statistics

Total hosts	MS03-11	MS04-013	MS05-001	MS06-013	MFSA2005-50	MS06-006
94	0	0	1	0	0	0
100.00 %	0.00 %	0.00 %	1.06 %	0.00 %	0.00 %	0.00 %

Total number of Exploited hosts is 1

Total Exploit efficiency is 1.06 %

Operation Systems statistics

OS name	Hosts	MS03-11	MS04-013	MS05-001	MS06-013	MFSA2005-50	MS06-006
Mac OS	1	0	0	0	0	0	0
Unknown	32	0	0	0	0	0	0
Windows 2000	9	0	0	0	0	0	0
Windows 98	2	0	0	0	0	0	0
Windows XP	50	0	0	1	0	0	0

Internet Browser statistics

Browser name	Hosts	MS03-11	MS04-013	MS05-001	MS06-013	MFSA2005-50	MS06-006
Firefox 1.0.7	1	0	0	0	0	0	0
Firefox 1.5.0.7	1	0	0	0	0	0	0
Firefox 2.0.0.3	2	0	0	0	0	0	0
MSIE 5.0	2	0	0	0	0	0	0
MSIE 5.01	1	0	0	0	0	0	0

Figure 8. Control panel of Webattacker

Comparative review of kits for installing malware through exploits

Here is a summary of all the features mentioned above:

Name	Programmed in:	Iframer	language	Recent exploits	Price
IcePack	Php +MySql	yes	Russian	Good	$400
MPack	Php +MySql	No	English	So so	$1000
Traffic Pro	Php +MySql	No	Russian	Not included	$20
Webattacker	Cgi	No	English	Poor	$20

Prices listed in the table usually vary depending on the forum and the seller. It is possible that some of these versions will be free in the future.

Vulnerabilities

Summary and trends

The effect of summer vacations can also be seen in the area of vulnerabilities. However, even though software and security companies are low on staff during these dates, it's a good time for certain independent researchers.

This quarter's most important vulnerabilities are as follows:

- MS07-036: Vulnerabilities in Microsoft Excel.
- MS07-039: Vulnerabilities in Windows Active Directory.
- MS07-042: Vulnerabilities in Microsoft XML Core Services.
- MS07-044: Vulnerabilities in Microsoft Excel.
- MS07-046: Vulnerabilities in GDI.
- MS07-050: Vulnerabilities in the Vector Markup Language.
- MS07-051: Vulnerabilities in Microsoft Agent.

Todas ellas permitirían la ejecución remota de código.

All allow remote code execution.

As we mentioned in the previous bulletin, vulnerabilities in the Office suite are on the rise, and this time around they are having a particular impact on Microsoft Excel. Remember that each security bulletin actually refers to several flaws, not just a single one.

MS07-036, for example, fixes the following vulnerabilities:

- CVE-2007-1756 – Calculation Error Vulnerability.
- CVE-2007-3029 – Worksheet Memory Corruption Vulnerability.
- CVE-2007-3030 – Workbook Memory Corruption Vulnerability.

All can be exploited remotely.

Moreover, there are two previously known components: XML Core Services and Vector Markup Language. Both have new flaws that can be exploited remotely through the browser.

Vulnerabilities

Evolution of remote vulnerabilities

An analysis of the vulnerabilities that have appeared this year shows a change in the area of remotely exploitable vulnerabilities.

In the past, the typical remote attack scenario consisted of a server with a vulnerable service and a client exploiting this vulnerability. Classic worms like Blaster reproduced in this way.

However, the current *modus operandi* has changed, mainly due to the fact that the means for accessing the Internet have also changed (there are now hardly any modem connections) and security policies have been reinforced with regard to remote connections on the most widely used operating systems.

At present, servers are not attacked directly, but clients are encouraged to access data on a server, and vulnerabilities are exploited in the client itself. This compromises computer security, as it is not longer sufficient simply to have a firewall to mitigate attacks.

Looking at this quarter's most significant vulnerabilities, it is clear that only one of them adheres to the old scheme: the Active Directory flaw. This is logical, as Active Directory is a component that runs on servers. As for the other vulnerabilities, they can be exploited either through the browser or by opening a specific document.

Software in the line of fire

Some software applications, like browsers or office software plugins are targeted by researchers as they allow remote attacks using the system described above.

This is manifest in products such as QuickTime for example, Apple has published patches in the last quarter for the following vulnerabilities:

Vulnerabilidades

- VE-ID: CVE-2007-2295 - Apple QuickTime JVTCompEncodeFrame Function MOV File Handling Overflow
- CVE-ID: CVE-2007-2296 - Apple QuickTime FlipFileTypeAtom_BtoN Function MP4 File Handling Overflow
- CVE-ID: CVE-2007-2392 - Apple QuickTime Multiple Media File Processing Command Execution Vulnerabilities
- CVE-ID: CVE-2007-2394 - Apple QuickTime SMIL File Processing Integer Overflow Vulnerability
- CVE-ID: CVE-2007-2397 - Apple QuickTime Multiple Media File Processing Command Execution Vulnerabilities
- CVE-ID: CVE-2007-2393 - Apple QuickTime Multiple Media File Processing Command Execution Vulnerabilities
- CVE-ID: CVE-2007-2396 - Apple QuickTime Multiple Media File Processing Command Execution Vulnerabilities
- CVE-ID: CVE-2007-2402 - Apple QuickTime Multiple Media File Processing Command Execution Vulnerabilities

All can be exploited remotely.

Unpatched Vulnerabilities

Two relatively serious vulnerabilities have been reported at the end of this quarter for which there are no patches available yet:

The first one is a stack overflow in the Microsoft Windows XP SP2 MFC42.DLL library. This library is normally used from ActiveX controls. Hence, any software that uses the library's vulnerable system can be used as an attack vector. Details about this vulnerability have been made public, but there is no information about the affected software.
At the moment, it has been confirmed that the flaw can be exploited through the following programs:

- HP All-in-One Series Web Release software/driver installer version 2.1.0.
- HP Photo & Imaging Gallery version 1.1.

Also, the GNUCitizen security blog has reported a critical vulnerability in Adobe Acrobat Reader. Details about it have not been made public yet, but Adobe is already working on a patch.

About Pandalabs

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

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