



# QUARTERLY REPORT PandaLabs (APRIL - JUNE 2007)

© PandaSecurity 2007

**PANDA**  
SECURITY

*One step ahead.*

# Content

<b>Introduction</b> .....	<b>3</b>
<b>The quarter day by day</b> .....	<b>4</b>
April 2007 .....	4
May 2007 .....	8
June 2007 .....	11
Highlight news .....	16
<b>Second quarterly figures</b> .....	<b>18</b>
Distribution of the new threats detected .....	18
Month by month .....	20
Threats detected by Panda ActiveScan .....	21
<b>Trends</b> .....	<b>22</b>
<b>Kits for installing malware through exploits</b> .....	<b>24</b>
What do they allow hackers to do? .....	24
How do they manage to infect users? .....	24
Mpack analysis .....	25
Which malware does it usually install? .....	26
How does it manage to infect so many web pages? .....	26
How often is it updated? .....	28
<b>The price of malware</b> .....	<b>29</b>
Most offered services .....	30
<b>Vulnerabilities</b> .....	<b>33</b>
Summary and trends .....	33
'In the wild' exploits .....	34
Unofficial patches .....	34
Apart from Microsoft .....	34
<b>About PandaLabs</b> .....	<b>35</b>

## Introduction

---

This report centers on the so-called 'Kits for installing malware through exploits', mainly focusing on Mpack. At PandaLabs, we have carried out a study about different tools available on the market.

We will continue with the second part of the article included in the previous report, in which we analyzed different services offered by cyber-crooks.

As usual, we will also talk about vulnerabilities. Towards mid-April, an exploit which allowed remote code execution using an ANI file vulnerability (animated cursor) hit the headlines. This reminds you that sometimes even the most 'innocent' element can be an attack vector.

Additionally, we present an article about the trends observed in the last few months, taking a look at the new attack techniques and those that have consolidated their presence.

There have been no alerts in this period. However, families such as Spamta or Cimuz have been quite active.

Curiously, we found a server which used the Cimuz Trojan and also hosted a program allowing its disinfection. It seems it was still being tested and the creator needed an easy way to disinfect the computers.

We hope you find the report interesting.

## The quarter day by day

---

### April 2007

#### Day 1:

Switzerland approved a new legislation to outlaw spamming.

#### Day 2:

Critical vulnerability in Windows allows attackers to remotely and silently run code through modified ANI files (mouse pointer icons).

#### Day 3:

Gary McKinnon, a hacker accused of entering hundreds of computers belonging to the Pentagon, the NASA, the army and the U.S. Air Forces for 18 months, will be extradited to the USA to be tried.

A group of hackers created an 'internal' instant messaging program called CarderIM, specifically designed to prevent authorities from monitoring or intervening on computers.

Microsoft broke its policy of publishing security advisories every second Tuesday of the month and published the patch for solving the ANI file vulnerability a week before, due to its seriousness.

#### Day 4:

Security experts confirmed that the WEP protocol, scheme to secure wireless networks, can be hacked between 50 and 95 percent of the time. They therefore recommend not using this protocol in especially sensitive networks.

#### Day 5:

Microsoft published a press release informing that some companies in Jordan have made millions of dollars through illegal low-cost software, originally destined for educational programs.

#### Day 6:

A survey carried out of 2,223 American adults revealed that 87 percent claimed to know Windows Vista, but only 12 percent would migrate to it in the next twelve months.

#### Day 7:

Three Japanese soldiers were arrested for exchanging confidential information. The soldiers claimed they were exchanging pornography and that confidential information was accidentally copied.

## The quarter day by day

---

### Day 8:

A group of hackers turn Apple TVs into computers. Hackers continue working to improve the computer features, and have caused great interest, having received 500,000 visits to their website.

Thailand joins the list of countries that block access to YouTube due to several offensive videos to the Thai monarchy.

Podsolo, the first virus for iPod was created, whose aim is to prove that a specific platform can also be infected.

### Day 9:

Canada carried out a simulation to check the reaction time against a cyber-attack and prevent the problems suffered in 2006.

### Day 10:

A woman offered her body in exchange for World of Warcraft credits, the famous online game. This is another example of the lengths to which people will go to get more privileges on online games.

### Day 11:

Microsoft published 6 security advisories, five of them considered critical, in its updates of every second Tuesday of the month.

### Day 12:

Microsoft sticks to its calendar and it looks like it will not sell more copies of Windows XP after the end of January 2008.

### Day 13:

A week after the DVD Security Group launched an update offering a solution for the exploit which allowed hackers to get disk passwords (HD, DVD and BD), several hackers announced they have also managed to overpass that protection.

### Day 14:

Microsoft announced that the flaws found in Word 2007 are not security flaws, but a program function, according to a company spokesperson.

### Day 16:

The image of Paris Hilton was used in emails as social engineering to infect users with the LoadImage exploit which exploits the vulnerability in ANI cursors.

## The quarter day by day

---

### Day 17:

According to ZDnet, the last 'Zero-Day' flaw implemented in the RPC interface on Windows DNS Server has been developed using information provided by Microsoft's security solutions section.

PandaLabs detected Artesimda.A, a Trojan that accesses files that store the information users enter in web forms. It also obtains remote access and total control of the affected computer.

### Day 19:

Up to the present, Microsoft has sold 244 copies of Windows Vista in China. This is due to increase in the one-dollar illegal sales of Vista copies.

A man and a woman were arrested by British police in Worcestershire for using their neighbours' wireless Internet connection. The fine for this same crime in 2005 reached 500 pounds.

Commtouch indicated that 90 percent of emails received are spam. Massive botnets are still the main means of worldwide spamming.

### Day 20:

Apple recently published a new update packet with 25 patches for Mac. To check the updates, Apple offers 10,000 dollars to anyone who manages to hack a completely updated Mac.

### Day 21:

Twenty year old Christopher Andrew Piasecki from Illinois, was accused of possessing child pornography on his computer and could face up to 10 years in prison and a 250,000-dollar fine if the judge finds him guilty of the charges.

### Day 22:

A hacker won \$10,000 in the CanSecWest security conference competition for accessing a Mac computer by exploiting a vulnerability in its Safari browser.

### Day 23:

PandaLabs detected Evilx.A, a Trojan programmed to connect to a specific web page to download malicious files including malware.

### Day 24:

A security flaw was detected in Google Calendar which allows users' confidential information to be accessed.

## The quarter day by day

---

**Day 25:**

PandaLabs detected Ridnu.C, a worm that writes romantic messages when users open the Notepad, switches the screen off every 5 seconds and opens the CD-ROM tray.

**Day 26:**

The Russian company IntelCore launched a utility tool that revealed OpenOffice document passwords to users who had forgotten their confidential data. This tool can obviously be exploited by intruders.

**Day 28:**

Google deleted sponsored advertising links since hackers used to buy key words searched in Google to fool users and redirect them to malicious web pages.

**Day 29:**

PandaLabs detected Dadlam.A, a Trojan that records users' keystrokes to obtain confidential data such as, user names, bank account passwords and email addresses, among others.

**Day 30:**

Adware and Trojans are the malware which most infections have caused in April, 27 and 25 percent respectively. The rest of the infections have been: worms (8%), backdoor Trojans (5%), dialers (4%) spyware (3%), bots (3%) and others.

## The quarter day by day

---

### May 2007

#### Day 1:

Italian hackers discovered the way to access computer systems and change the traffic alerts by sending false FM radio signals, causing fake accidents and traffic jams.

#### Day 2:

Crackers replace DoS attacks with spamming, since the latter is less dangerous and much more lucrative economically.

PandaLabs detected Wsnpoem.AW, a Trojan that monitors Internet traffic and captures information entered by users on certain web pages.

#### Day 3:

U.S. police arrested a Chinese kid accused of being a terrorist threat, for creating a virtual map of his school for an online game of Counter Strike.

PandaLabs detected Banker.HIK, a Trojan that displays fake access windows when users visit web pages of specific Brazilian online banks.

#### Day 4:

PandaLabs detected Cimuz.FH, a Trojan that steals information from the computer, such as, IP and email addresses, computer names, etc., stores the data in a text file and sends the information to a specific server.

#### Day 5:

PandaLabs detected MSNDiablo.A, a worm that disables the Windows Registry Editor and the Task Manager, and spreads through MSN Messenger.

#### Day 7:

A Russian teacher was sentenced to pay €143 for using pirate Microsoft software in his classroom. The teacher will appeal claiming he was unaware the software was illegal.

#### Day 8:

Microsoft published security advisories to fix 19 security flaws, from which 15 are considered critical. This time the patches are aimed at its office suite.

PandaLabs detected Grum.D.drp, a virus that infects executable files on the computer. It also has a mail server from which it can send spam.

## The quarter day by day

---

### Day 10:

German police investigate Second Life after discovering that “virtual kids” have been abused in the virtual world. It seems like there is a group of people who pay money for maintaining virtual sexual experiences, punishable under German law.

### Day 11:

According to rumors, the new version of Microsoft’s “LongHorn” operating system will be called “Windows Server 2008”.

### Day 12:

An executive at McAfee has been found guilty of 15 security frauds and could be sentenced to 150 years in prison and a 15 million-dollar fine.

### Day 14:

An investigation conducted by Google estimates that approximately 10 percent of the websites users visit could damage the PC, since they host malware. Google will therefore create a blacklist of insecure and dangerous sites.

### Day 15:

The US Justice Department will increase the number of attorneys trained to prosecute intellectual property (IP) crimes and will use all the tools possible to win the war against software and music piracy.

### Day 17:

Today is Internet Day. Internet is calculated to have over 1,000 million users worldwide, which is the equivalent of 16.8% of the population.

### Day 18:

The headquarters of the PP and PSOE Spanish political parties in Leon and Oviedo were set on fire in the virtual world Second Life.

### Day 19:

Estonia asks NATO to investigate the cyber-attacks banking and political party web pages among others, have been receiving for three weeks, and take the necessary measures.

### Day 20:

After reporting that 235 of its patents were being copied by operating systems such as Linux, Microsoft has stated it will not take any legal actions against Linux for the moment.

## The quarter day by day

---

### Day 21:

Microsoft has managed to sell its software to the Vietnamese government, ending a long battle to eradicate illegal software in the communist country.

Polish youngsters were accused of subtitling films and series downloaded from P2P networks. Ten PCs, seven laptops and over 2,000 CDs which allegedly contained pirate films and software were also requisitioned. Consequently, they face up to 2 years of prison.

### Day 22:

PandaLabs detected Ridnu.D, a worm that writes romantic messages when users open the Notepad and displays the "MR COOLFACE !" message when the Run option in the Start menu is accessed.

### Day 23:

Sam Peterson was arrested for accessing the Wifi service a café offered its clients from his car. Peterson could face up to 5 years in prison and a 10,000 dollar fine in the state of Michigan for not entering the café to order a cup of coffee.

PandaLabs detected Conycspa.AJ, a Trojan that changes the results of several browsers including Google and Yahoo!, when users search for specific medicine.

### Day 24:

Sources close to Microsoft have confirmed the launch of Windows XP Service Pack 3, but it looks like it will not arrive before 2008.

### Day 25:

USA evaluates whether to tax Internet access. The state and local government pressure groups are in favor of the tax, which could provide them with a good source of money.

### Day 30:

PandaLabs detected Bankey.A, a password stealer Trojan which obtains user data to access banks. To do this, it displays a spoof banking web page which requires access data.

## The quarter day by day

---

### June 2007

#### Day 1:

Firefox 2.0.0.4 allows bypassing the content filtering in Windows Vista and downloading Internet files that should be blocked.

#### Day 3:

A 'man-in-the-middle' attack was published which exploited a vulnerability in the Google Desktop bar, allowing programs installed on victims' computers to be run.

#### Day 4:

A new phishing scam appeared which requested bank details to theoretically refund €121 to users due to a debiting error.

Hackers' failed attempt to infect Sunbelt using highly customizable emails to fool employees into running the attached file containing malware to steal data.

#### Day 5:

Security expert Michael Zalewski found 4 security holes in Internet Explorer and Firefox. One of the vulnerabilities affecting versions 6 and 7 of Internet Explorer is considered critical.

PandaLabs detected the worm MSNHideOptions.A, which changes the Internet Explorer home page, hiding desktop icons and the clock in the notification area.

#### Day 6:

Intellectual Weapons offers security investigators the opportunity to patent the patches produced to fix vulnerabilities.

#### Day 7:

The documentation download for the automated Windows installation Kit in Microsoft's Winbeta zone, which seems to include support for Windows Server 2008 and Windows Vista SP1, augurs the launch of the first Windows Vista Service Pack.

A programming flaw in Yahoo Messenger allows remote execution of arbitrary code.

## The quarter day by day

---

### Day 8:

A new malware threat called 'Roberto' appeared, which resends itself by email to MSN Messenger contacts of the affected computer.

A study revealed that the sites for downloading music contain more malware than the ones that host pornography.

### Day 9:

Two Springfield (U.S.) citizens were arrested for scamming over 684,000 dollars from some 9,700 victims, using a website leading them to believe they would receive 38% daily benefit in their investments.

### Day 10:

PandaLabs detected SpreadBanker.A, a worm programmed to steal passwords for accessing several online banks and computer games.

It also decreases computer security, as it ends antivirus and firewall processes and prevents users from accessing specific security-related websites.

### Day 11:

A study by Forrester Research reveals that in 2008 there will be over a thousand million PCs worldwide, and that by 2013 this figure could double, due principally to technological development in Brazil, Russia, China and India.

### Day 12:

Several anti-spam sites (Spamhaus, Spam URI Realtime Blocklists and Realtime URI Blacklist) have suffered DDoS attacks for 3 days via a 'zombie' network.

Computers with anti-DDoS systems were not affected.

### Day 13:

Microsoft published its security bulletin which corrected 15 security flaws, 9 of them critical. Most critical flaws appear in Internet Explorer 7 and Vista, and are caused by problems in ActiveX controls which allow taking remote control of the affected computer.

### Day 14:

The U.S. Justice Department and the FBI confirm via a report that they have found over a million computers affected by a worm-type malware that creates huge botnets.

## The quarter day by day

---

### Day 15:

Yahoo fixed a cross-site-scripting attack (XSS) which allowed total access to users' accounts if they clicked a harmless-looking link.

### Day 17:

PandaLabs detected the Moaphie.A worm, which spreads through MSN Messenger and the available system drives. It also disables functions like the Run option in the Start menu, the contextual menu, and applications like the Task Manager and the Windows Registry Editor.

### Day 18:

After a 7-month long police operation, German police have arrested 111 people accused of organizing scams. They made victims believe they had won a lottery prize and requested money for handling costs.

### Day 19:

A new version of Mpack was discovered: 0.90. This malicious application accesses web pages to trace vulnerabilities on computers and downloads a corresponding exploit the moment it detects any vulnerability on a user's computer.

PandaLabs detected the Suarabh.A Trojan, programmed to capture users' keystrokes and obtain confidential data, such as passwords or user names.

### Day 20:

PandaLabs detected Dreamsystem, a tool which allows hackers to control botnets of the Dreamsocks family. The latest known version is 1.3, which can be bought for 750 dollars.

A Trojan called Harrenix.A has appeared, which passes itself off as the "Harry Potter and the Order of the Phoenix" trailer in Italian. When run, it displays a message saying that an error has occurred while reproducing the video. Meanwhile, it downloads Dialer.KJD.

### Day 21:

In the last two years, the U.S. National Security Department has suffered over 800 hacking attacks, virus infections and other computer security problems.

## The quarter day by day

---

### Day 22:

The Pentagon was forced to leave 1,500 computers offline as a preventive measure, after detecting a hacker intrusion in the email system.

### Day 23:

Microsoft patched 12 out of 27 Vista vulnerabilities in the six months following its launch, while 36 out of 39 XP vulnerabilities were corrected in the six months following the XP launch.

### Day 24:

A 28-year old was arrested in Valencia for launching a virus for high-range cell phones which has affected around 115,000 people and has caused losses running into the millions to operators and users.

The Spanish General Data Protection Register will analyze the way in which Internet browsers store the data of searches made by users to make sure the relation between users and the data searched is not recorded.

### Day 25:

A hacker threatens to publish 40 vulnerabilities which theoretically allow malicious code execution if Google does not immediately solve the security holes found in Youtube.

PandaLabs detected a new worm, Gronev.A, which shuts Internet Explorer down every time it detects the word Search in the address bar. When run, it also plays a song using Windows Media Player.

### Day 26:

A 17-year-old boy was arrested for hacking and closing the website of Belgian police. The note he left after the attack indicating his age was a determining factor for his quick arrest.

### Day 27:

A study done by the security commission of the Internauts Association, informs the National Police and the Civil Guards that they have found several servers prepared to host fraudulent websites of Spanish financial entities.

## The quarter day by day

---

### Day 28:

The hacker who in 1999 bragged about controlling the twenty biggest software pirate sites has been sentenced to four years in prison. The hacker was arrested in 2001 and spent three years in a preventive prison in Australia before being extradited to the U.S.

PandaLabs detected the Botvoice. A Trojan which does not allow running files with BAT, COM, EXE and MP3 extensions among others.

Once it affects a computer, it continuously repeats:

"You has been infected I repeat You has been infected and your system files has been deletes. Sorry. Have a Nice Day and bye bye".

### Day 29:

Microsoft's website in the United Kingdom has suffered an attack which has changed the aspect of some of its pages. The action seems to have been carried out from Saudi Arabia.

## The quarter day by day

---

### Highlight news

#### A hacker could face up to 70 years in prison

Gary McKinnon, the British man who allegedly carried out the most important military hacking act in history, has been unable to avoid extradition to the U.S.

McKinnon allegedly attacked 97 American computers both military and belonging to the NASA, during 2001 and 2002.

When extradited to the U.S., he will probably face a military court and potential internment in Guantanamo Bay. If he is found guilty, he could face 70 years in prison.

McKinnon wants to be tried in the United Kingdom since the alleged attacks took place there, and still states he was only seeking evidence of UFO activity.

#### Arrested for providing free film subtitles

The huge traffic that ed2K or BitTorrent network films generate has caused a significant increase in the number of users who create subtitles for those films and series. As incredible as it may sound, providing subtitles could land you in prison.

That is exactly what has occurred to at least six people in a Polish group who translate and write film and series subtitles. The illegal trade of these translations and subtitlings is forbidden under Polish law. Polish police worked together with German police – since the servers were hosted in this country – to arrest the people who had committed the 'crime'.

The website Napisy.org was immediately shut down and the people involved were questioned. Ten PCs, seven laptops and 2,000 CDs which probably contained pirate films and software were also requisitioned.

The people accused with ages ranging from 20 to 30, could be sentenced, in the worst case, to 2 years in prison for publishing illegal material with copyright.

## The quarter day by day

---

### Highlight news

#### Be careful with open Wi-Fi networks

It is increasingly common when nearing public places, mainly transport stations (trains, buses, planes, etc.) for cell phones to inform you that departure time tables are available via Bluetooth.

The need to be informed can let you be off-guard and be exposed to attacks against your privacy almost voluntarily. The Better Business Bureau organization (BBB) recently warned the public about this.

Remotely working with a laptop is a daily task for someone who is continuously on the move while working, that is why the number of airports offering open Internet connection via Wi-Fi is increasing. Work instead of waiting.

Hackers are aware of this and are starting to establish their own open networks in these places. It is easy to call your connection 'Open connection'. What potential victims do not know, is that all the traffic generated will automatically be filtered for passwords or other sensitive data while they browse. And if they have any shared drives, their files could be exposed.

The recommendations below could be handy in these cases:

- Do not rely on the networks available and avoid automatic connection.
- Disable shared resources (folders, etc.) when using wireless networks.
- Remember that the use of VPNs, virtual private networks, is the safest for connecting with your work.

#### First Spanish person arrested for creating a cell phone virus

Police in Valencia arrested the first Spanish person accused of creating and spreading malware for cell phones. The 28 year-old distributed up to 20 different viruses affecting approximately 115,000 people.

The cyber-crook used the known Cabir and CommWarrior viruses which affect Symbian terminals, and spread them through multimedia messages via Bluetooth.

Due to cell phone expansion and migration towards more complex systems like Symbian, cell phones have become a target for malware creators. It is therefore a matter of time before manufacturers start to focus on cell phone security.

The police managed to arrest the hacker and confiscated huge amounts of computer materials and up to nine high-range cell phones.

## Second 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 second quarter of 2007:

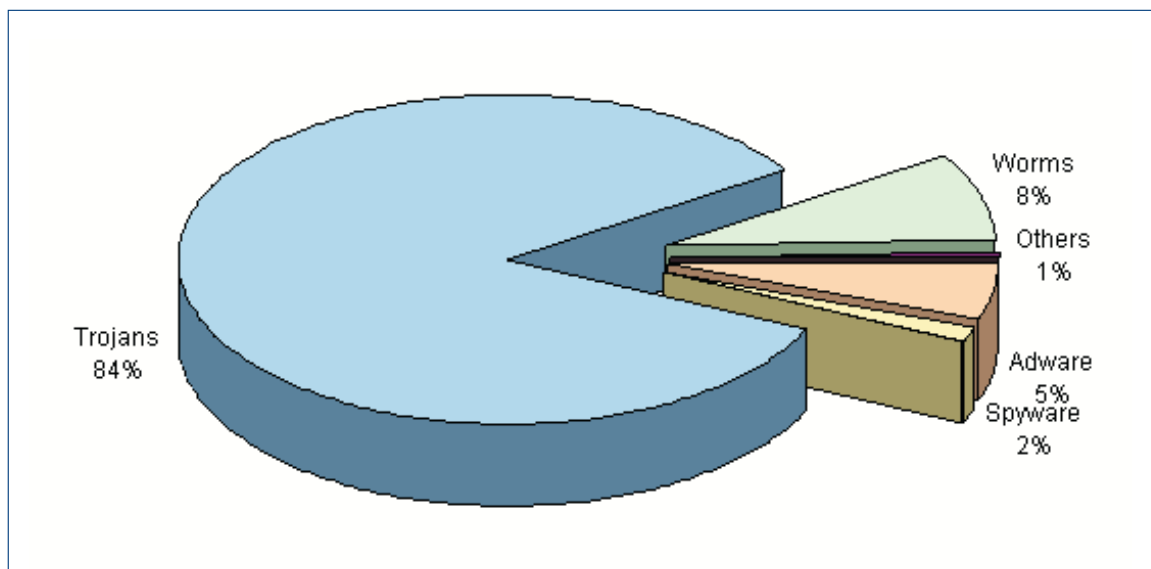


Figure 1. New malware variants detected by PandaLabs.

Trojans, which have gone from 74% to 84%, are clearly the predominant malware category in this quarter. Worms have decreased 5% due to malware creators' preference in carrying out more silent and selective attacks using Trojans.

Trojans rise as opposed to worms' has been influenced by Mpack-type tools, which manage to infect systems by exploiting vulnerabilities, without the need for malware to auto-distribute itself. Compromised computers can be used to create botnets, to later, send spam, spread additional malware, carry out DDoS attacks, etc.

The sub-category of Backdoor Trojans is also included. Bots are integrated in worms or Trojans according to their nature.

Adware and spyware combined accounted for 12% of infections last quarter and 7% this quarter.

## Second quarterly figures

Categories with little relevance have been grouped in the 'Other' category.

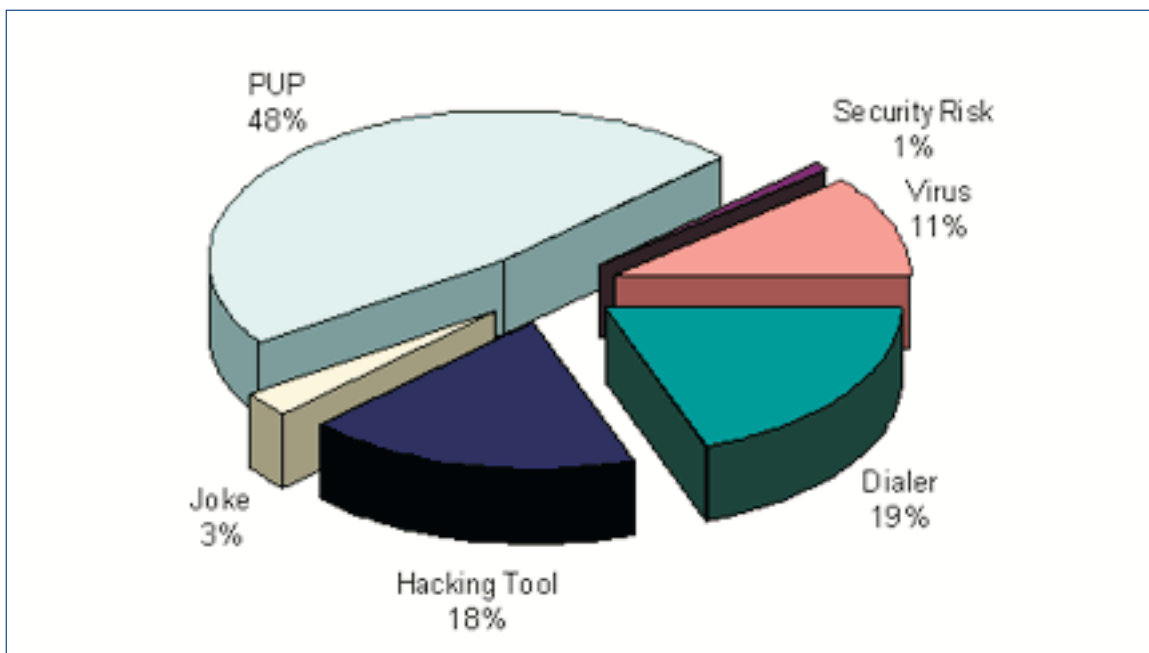


Figure 2. Classification of the 'Other' category.

It is worth mentioning that PUPs (Potentially Unwanted Programs) have increased 14% in this quarter.

The noticeable decrease of viruses, from 26% at the beginning of the year to a current 11%, is due to the fact that malware creators no longer seek such notoriety or system breakdowns. Current malware is generally aimed at financial gain.

Although dialers tend to decrease, thanks to the increase in broadband services, they remain at 19%.

## Second quarterly figures

### Month by month

Below you can see the appearance of new malware month by month, separated into the most important categories. The growth of Trojans is constant.

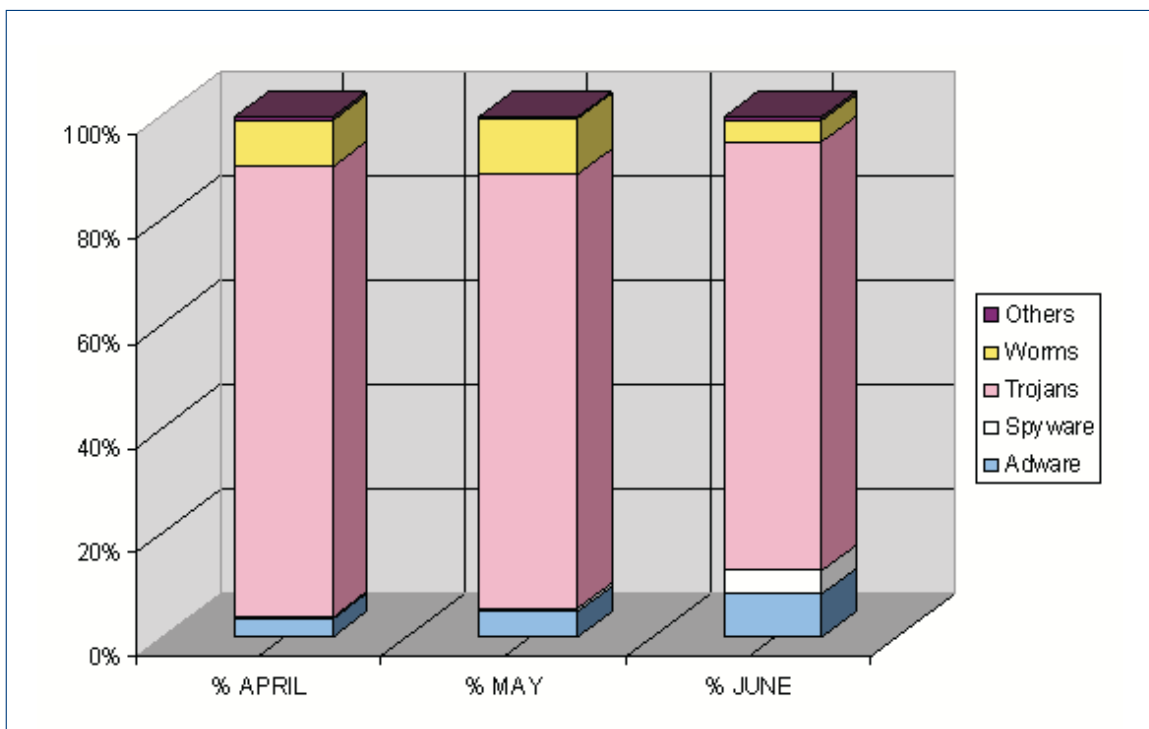


Figure 3. Appearance of new malware.

## Second quarterly figures

### Threats detected by Panda ActiveScan

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

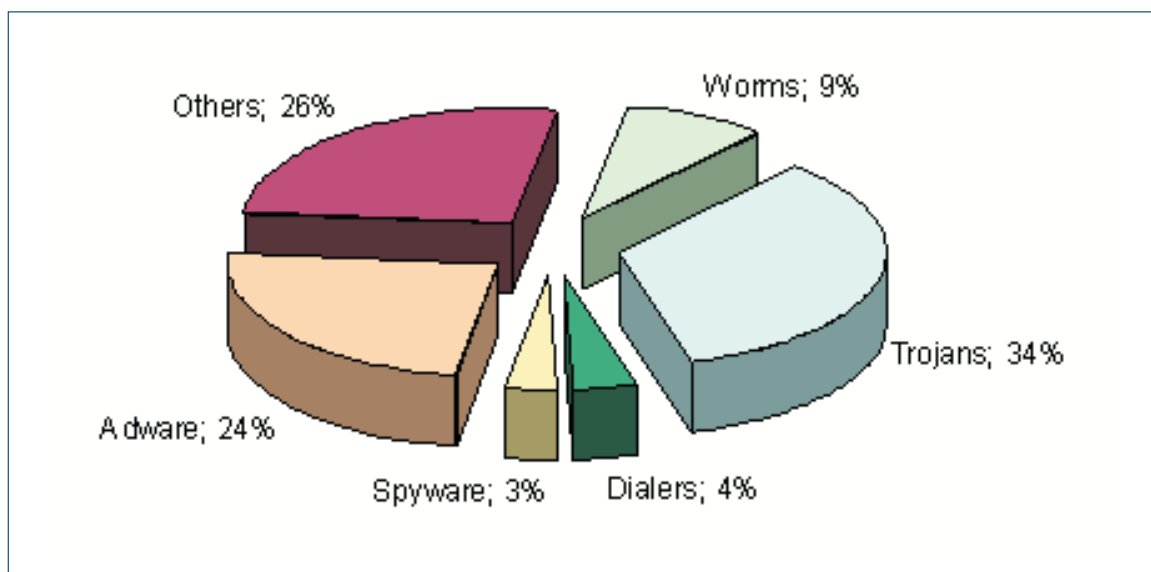


Figure 4. Detections carried out by Panda ActiveScan.

Trojan detections have risen from 31% to 34%.

Dialers have gone from 5% at the beginning of the year to 4% at present.

The categories of adware and spyware combined accounted for 27% of detections, a slight drop with respect to the last quarter.

## Trends

---

In general, there have been no major changes in trends compared to previous quarters. Malware continues to expand rapidly. More malware has been detected in this quarter than between 2000-2004.

There continues to be vulnerability-related alerts, mainly due to vulnerabilities found in ANI and WMF files.

Professionalization among malware creators can be seen in the type of tools used and the way in which they are exchanged. As described in the article "The price of malware", some competitors presently swap knowledge, tools and products.

In previous studies, we detected tools that controlled tens of thousands of web pages. Once the investigation was carried out, we thought that an application was being used to automatically infect all the pages hosted on the same vulnerable server.

Consequently, as in the past months, the principal means of infection is still shifting from email to web hosting. As the number of worms and viruses capable of infecting and spreading decreases, the number of servers with malware, mainly Trojans, increases. This offers malware creators more control to select the type of malware and limit the number of infected users.

Additionally, "typosquatting", the technique that consists in buying domains which resemble known brands' and which infect users when they enter the wrong address in browsers, is still in use. Search engines with sponsored results are also beginning to be used to increase infection possibilities. Some of the most searched for words are selected and a link to the compromised server is bought.

Since the amount of information malware is capable of collecting is increasing, scanning the data becomes a problem. Together with professionalization, servers appear that use modules to scan the data and ease exploitation.

Once again, social engineering proves its effectiveness by exploiting the launch of Hollywood blockbusters, such as, Pirates of the Caribbean or Harry Potter. The technique consists in sending a link to a web page which pretends to download a promotional video.

## Trends

---

New versions of operating systems and common-use tools are also being exploited to confuse users and distribute malware. Files exchanged in P2P networks are still a common source of infection.

Email phishing attacks are progressively being replaced by specialized banker Trojans. The inclusion of anti-phishing bars in main browsers and improvements in anti-malware tools has increased protection against classic phishing.

Some Trojans are also beginning to use the Background Intelligent Transfer Service (BITS) used by Windows to update operating systems. This way, connection can be established with the outside, dodging the firewall. The most common are the downloader Trojans, who use it to transparently download new malware onto infected computers.

Some Trojans use this service to send stolen data. In this aspect, it is worth mentioning that although it is an original and quite effective way to dodge perimeter security solutions, it requires prior infection, which is not an easy task.

## Kits for installing malware through exploits

---

Numerous web pages are currently used to infect users with malware through exploits. They tend to exploit the latest vulnerabilities; presently, the most often used are MDAC (MS06-014) and .ANI (MS07-017).

Some of these web pages use a single exploit to infect users. The possibility of infecting many computers is therefore slim. That is why the so-called "Kits for installing malware through exploits" have appeared, which increase infection capacity. This is due to the fact that these kits first check the type of computer to infect and search for the most appropriate exploit to infect it.

These kits can be old, such as Web-attacker or more recent, such as Mpack, Neosploit or eCore exploit pack.

### What do they allow hackers to do?

They allow hackers to automate computer infections and distribute all types of malware. Some of these kits allow hackers to select or exclude geographic areas to infect.

### How do they manage to infect users?

Below are some of the techniques used:

- Hack web page servers. To do this, they usually add an iframe-type reference at the end of the file which the site loads by default, and which points to the location where the kit is installed. Apart from adding links to sites, they usually use servers to store the kit or other types of malware. This way, they are much more difficult to locate.
- Enter certain words on the web pages where they are stored, so that when the web page is indexed in the browsers, users end up at the page and get infected.
- Buy domains with similar names to known sites users tend to access. For example, gookle, which only differs in a character from the famous google browser. Users who wrongly enter a character in the browser name could be infected.
- Send massive emails to numerous addresses. These emails usually contain links and use social engineering techniques to be run. The Trj/Goldun and Trj/Haxdoor families frequently use this technique.
- Buy sponsored links from Google for certain search words.

# Kits for installing malware through exploits

## Mpack analysis

We carried out a study about Mpack in April and May which revealed surprising data: we located 41 servers with Mpack installed, from which over 1,217,000 users were infected, and found 366,717 links on web pages from which Mpack could be installed.

Mpack is an application that is installed on the server and allows malware to be run on remote systems using several exploits. As new exploits appear, new program updates are released to infect as many computers as possible.

See the tables below which correspond to Mpack’s statistics panel, to get a broader view of its scale:

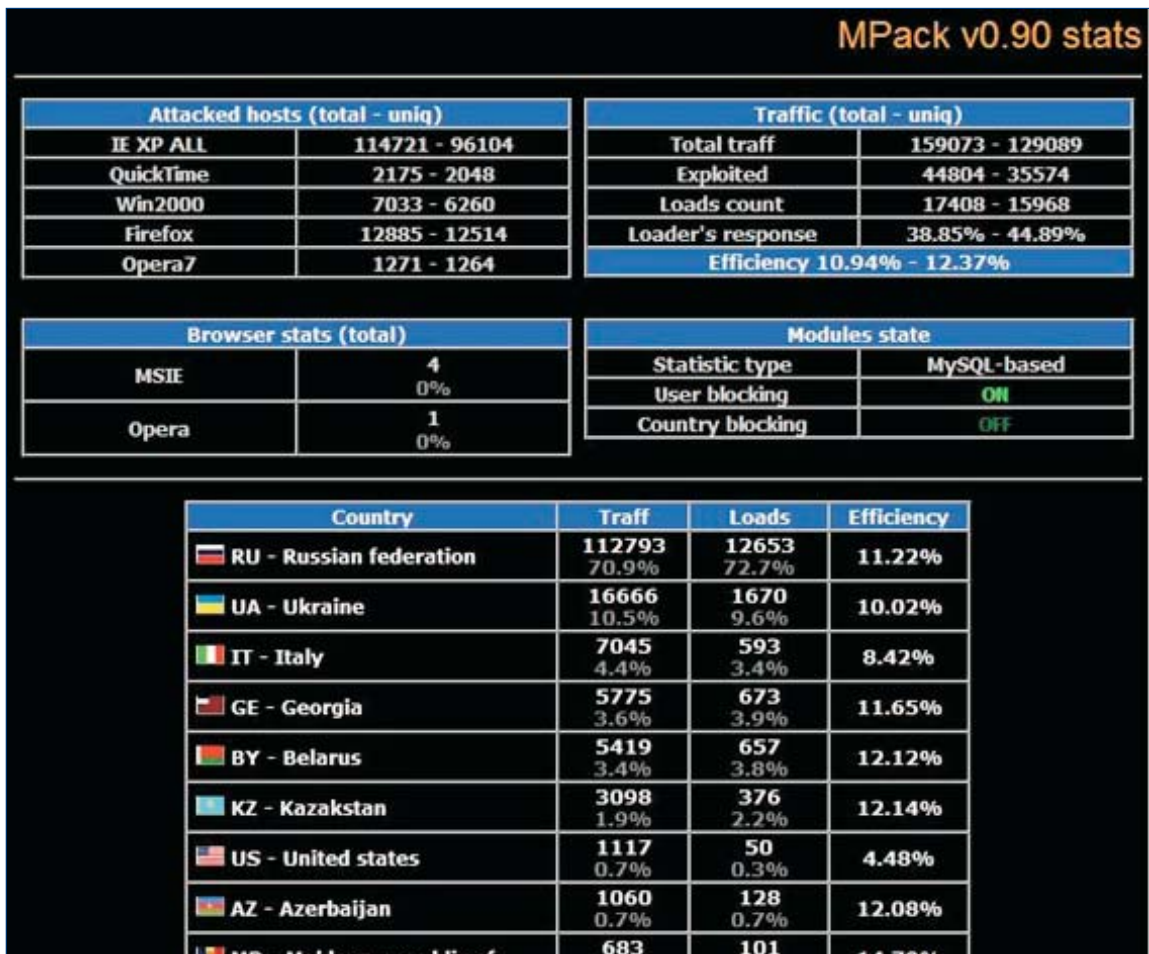


Figure 5. Mpack’s stats module.

## Kits for installing malware through exploits

---

Mpack's stats panel informs about: the number of computers attacked per product whose vulnerabilities they tried to exploit (top left), infection efficiency rate of computers that visited the web page containing the kit (top right), visits to the web page per country and their corresponding infection success rate.

### Which malware does it usually install?

It usually installs other bot kits or banker Trojan kits on sale. The most common are:

- Trj/BankoLimb (Limbo)
- Trj/Briz (VisualBreeze o VisualBriz)
- Trj/Sinowal
- Trj/Snatch: Steals users' bank details.
- Trj/LdPinch (Pinch): steals all sorts of data.
- Bck/Barracuda
- Bck/DreamSocks (Dream System): Allows hackers to launch DDoS attacks.
- Bck/Zunker (Zunker): sends messages with a link to a malicious page.

### How does it manage to infect so many web pages?

It is unlikely or impossible, for those 366,717 websites to have been hacked and infected manually. We found out that they use Iframers, programs that allow automating massive website infections.

To infect websites they search for the site's home file (usually index.php, index.htm, index.html, etc.) and they add an iframe field on the web page pointing to the website where Mpack is installed.

To access the web page, the Iframers usually indicate the user name and password of the FTP server where it is stored.

Below are some options that Iframers allow attackers to carry out:

- Add the iframe field at the beginning or end of the file.
- Show up-to-date information of the number of servers infected.
- If administrators delete the iframe field, it infects the website again by adding the iframe.

These Iframers obtain FTP accounts via hacked websites or through information collected by malware installed on infected computers.

## Kits for installing malware through exploits

Due to the vast amounts of data collected, they use a tool called "PHP script that validates ftp accounts" which is used to extract valid FTP accounts.

The graph below shows the process carried out by Mpack and other "Kits for installing malware through exploits":

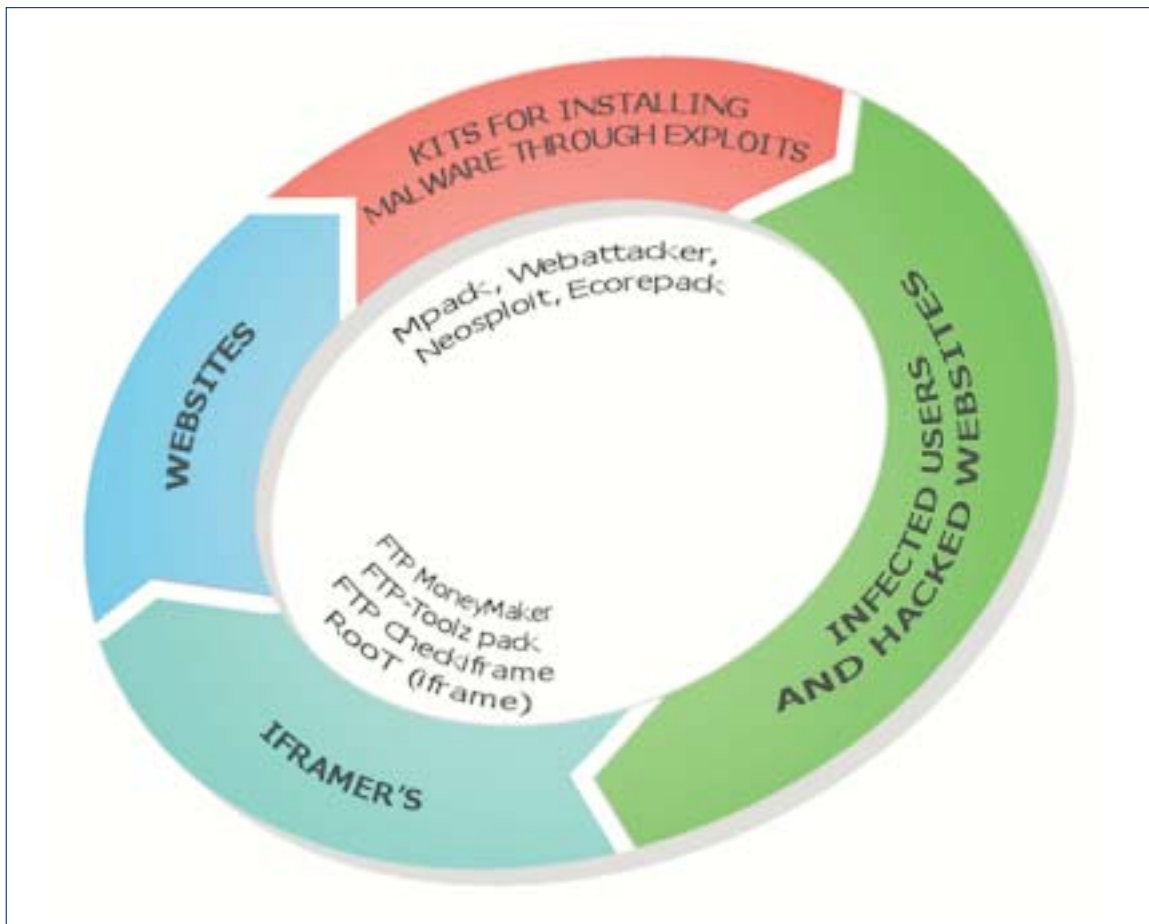


Figure 6. Representative graph of the infection process

## Kits for installing malware through exploits

---

1. Users are infected by “kits for installing malware through exploits” when they visit specific websites.
2. The malware installed steals information from users’ computers and hacked websites.
3. Iframers use the passwords obtained from users to infect more sites. Return to point 1.

### How often is it updated?

Kits are updated every time new exploits appear to take advantage of new vulnerabilities.

Occasionally versions are published which include improvements to the data management, graphic interface or installation or, in which the exploit encryption has been modified, etc.

Based on our research, we could say that a new version is published every month.

## The price of malware

---

It is a confirmed trend: activities that develop around malware are becoming a highly lucrative business. Cyber-crime is increasingly widespread as organizations emerge which use all types of resources to obtain financial profits by using malware.

Traditional virus creators are left behind, since it is now money that draws this business. Organized groups of cyber-crooks are undergoing specialization and professionalization, offering specific services and obtaining the necessary tools to become more effective.

Factors like legal impunity make it easier for criminal organizations to operate, since most of these groups come from countries with little or no legal regulations in this field. Professionalization in this sector has also led to specialization: malware creators, distributors and exploiters, they all shape the channel needed for the business model to work.

Nowadays, there are authentic malware markets where services and products are bought and sold. Several profile-types converge in them: groups that control large botnets, programmers that offer their own Trojans, credit-card sales or official document falsification, etc. In these markets, specific Trojans for stealing information can be bought and denial of service attacks against companies can be contracted.

Here we describe some of the most common services:

## The price of malware

---

### Most offered services

#### DDoS attacks

Botnets are used (traditional, like IRC, or more modern, like HTTP). This service is very cheap, a ten-minute trial DDoS attack can even be contracted before purchasing it.

DDoS attacks	
Attack duration	Cost
1 hour	\$10-20
2 hours	\$20-40
1 day	\$100
> than one day	Over \$200

#### Spam

Spamming can be done by using botnets or by purchasing lists of millions of email addresses.

Spam	
Services offered	Cost
Spam housing	\$200
Server used for spam	\$500
> 10 million messages a day	\$600

## The price of malware

Lists of email addresses to send spam to				
Number of email addresses	Cost per country			
	USA	Germany	Russia	Ukraine
1 million	\$100	\$100	\$100	\$100
3 million	\$200	\$200	\$200	\$200
5 million	\$300	\$300	\$300	-
8 million	\$500	\$500	\$500	-
16 million	\$900	-	-	-
32 million	\$1,500	-	-	-
32 millones	1.500\$	-	-	-

### Sale of information

Among the services provided are: sale of personal information, sale of banking information, etc. Bear in mind that this information is usually obtained by using botnets, which download Trojans (usually banker Trojans) to steal data. We have grouped all stolen accounts together, from email or FTP accounts, to accounts for online shopping.

Limbo Trojan	
50 MB of logs (they contain email accounts, FTP, credit cards, online banking information, etc.)	\$30

### Hacking jobs

Websites, business networks, etc. are offered all sorts of hacking jobs. It is usually the buyer who requests the services and offers to pay. The most common services are: to obtain FTP or email accounts, or to collapse companies' servers.

### Official documents

According to our data, some sellers offer all types of official documentation, from passports to permits, including driving licenses or work permits.

## The price of malware

---

### Banking information

Millions of bank accounts are obtained by exploiting botnets. Some groups offer to create credit cards using this information, although buyers usually use this data to buy domains and create botnets or other resources to offer new services.

### Software

Sale of all types of malware: from viruses and Trojans to HTTP bot management tools, encryptors, log managers of HTTP bot management tools, Trojan creators, etc.

Other software	
Description	Cost
Mpack (exploits vulnerabilities and installs Trojans when visiting websites who have it installed)	\$1,000
Limbo (tool for managing HTTP bots)	\$500
Trojan for webmoney (captures webmoney accounts)	\$500
Dream System (to collapse servers)	\$750
Pinch (Trojan creator)	\$30 per Trojan
Joiner (to conceal executable files)	\$30

We are unaware of the scope and the relationships between the different groups of cyber-crooks who control this market, even though they all offer their services in specific forums which are easy to locate and access. Most of these markets are located in Eastern European countries, Russia being the country which offers most services.

The buyer profile responds to small groups, who aim at obtaining financial profits using previously bought tools for: spamming, carrying out DDoS attacks, buying and selling information, etc.

Given the existing competition to sell the same service, for business to be profitable, they often offer discounts and use other marketing techniques, like trying the service before it is purchased.

# Vulnerabilities

---

## Summary and trends

Two words have been present in the vulnerability environment this quarter: ANI and DNS. More specifically:

- MS07-017: Vulnerabilities in GDI could allow remote code execution.
- MS07-029: Vulnerability in Windows DNS RPC interface could allow remote code execution.

The first (MS07-017) affects the format of animated cursor files. It stems from a flaw in the structure and can be remotely exploited, since these cursors can be inserted into Internet documents.

In fact, it is a variant of a previously solved vulnerability:

- MS05-002: Vulnerability in cursor and icon format handling could allow remote code execution.

The second vulnerability (MS07-029) exploits a flaw when processing a request to the Windows DNS RPC interface. It can be remotely exploited and poses a high risk to servers. Note that regardless of the new protection technologies introduced in Windows 2003, a functional exploit was implemented in the operating system.

Other significant vulnerabilities in this quarter are:

- MS07-018: Microsoft Content Management Server.
- MS07-019: Plug and Play universal.
- MS07-020: Microsoft Agent.
- MS07-021: CSRSS. All allow remote code execution.
- MS07-022: Windows Kernel: vulnerability which could allow elevation of privilege.

As in the last quarterly report, the number of vulnerabilities that affect Microsoft Office products is still increasing.

Below you will find a list of the most important:

- MS07-023: Vulnerabilities in Microsoft Excel.
- MS07-024: Vulnerabilities in Microsoft Word
- MS07-025: Vulnerabilities in Microsoft Office.

All allow remote code execution.

## Vulnerabilities

---

### 'In the wild' exploits

The fact the two most important vulnerabilities this month have been detected 'in the wild' (i.e. active and being used) is worrying.

- The ANI file format vulnerability was discovered by McAfee Avert Labs in a forum as a proof-of-concept. We do not know whether this is public or private, although Microsoft was already aware of the flaw. What's more, they had already been working on the patch for some time, since the Determina Research team had informed them about it.
- In the case of the DNS/RPC vulnerability, Microsoft received the warning of a possible exploit for an unknown vulnerability in this service, probably due to a targeted attack. A few days later, Microsoft published the security advisory and public exploits for the vulnerability started to appear.

### Unofficial patches

Due to the time it takes to develop patches, third-parties are starting to publish unofficial patches.

Regarding the ANI file format vulnerability, it was eEye and ZERT who created a workaround to prevent these attacks.

### Apart from Microsoft...

On May 29, Apple published some patches which affected several of its products, the most critical possibly being:

- Buffer overflow vulnerability in Apple Mac OS X mDNSResponder: could allow remote code execution.

The vulnerability is located in the UPnP IGD service. A public exploit is available and it can only be exploited in local area networks.

## About PandaLabs

---

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

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