



G DATA

Malware Report

Semi-annual report January-June 2008

Ralf Benz Müller & Thorsten Urbanski

Go safe. Go safer. **G DATA.**

G DATA Malware Report January-June 2008

Ralf Benzmüller & Thorsten Urbanski

1. Summary:

Explosive growth of malware

In 2008, the consolidation phase of the malware industry is bearing its deadly fruit. 2007 was deemed to be a record year for malware with a growth rate of 300 percent compared to 2006, but 2008 is already breaking all the records. In the first three months of this year alone, more malicious agents were circulated than in the entire previous year (133,253).

Therefore we are not expecting the flood of malware to recede. G DATA Security Labs estimate that there might be half a million new malware agents in the 3rd quarter of 2008 alone - this would signify a growth rate well above 400 percent.

Data theft and interconnection of hijacked PCs into botnets are the criminals' primary goals, going by analyses of malicious code families. Hence downloaders (37,546) and backdoors (44,156) represented the majority of newcomers in the first half of 2008.

Malware	Newcomers	Proportion in percent
Backdoors	75.027	23,6 %
Downloader/ Dropper	64.482	20,3 %
Spyware	58.872	18,5 %
Trojan horses	52.087	16,4 %
Adware	32.068	10,1 %

Table 1: Top five malware January to June 2008

1.1 Minefields on the net

The threat from primed websites has increased markedly. The expansion of malware across the Internet predicted by G DATA in 2007 has long since become reality.

Perpetrators use this technique to exploit security holes in browsers or browser plug-ins such as Flash applications or Adobe Acrobat Reader, for example. Contrary to long-held assumptions, these dangers do not normally lurk in the "red light districts" of the Internet but can for the most part be found on popular websites.

1.2 Smartphones: marketing bubble burst

The hype surrounding smartphone viruses is not reflected in the current figures: only 41 new malware agents were brought into circulation by malware authors up to the end of June 2008. Most of these malware programs are semi-legal monitoring software or proof-of-concept studies, according to G DATA studies.

This becomes even clearer if you look at the total figures for new smartphone malware agents since January 2006: 145 new malicious agents for all smartphone operating systems. It would be excessive to speak of a real danger for owners of such devices at this point in time.

1.3 Conclusion and forecast

According to G DATA estimates, we cannot expect the malware industry to take a summer break over the coming weeks and months. The output of new malware will increase further and might reach totally new dimensions.

Upcoming major sporting events such as the Beijing Olympics, for example, could well make the situation even worse. Online criminals use global events as hooks that they can use to reinforce their hunt for data and increase money-making opportunities. Hence, an increased output of malicious mail is to be expected soon.

Smartphone viruses, on the other hand, will hardly play any role this year. This is either because the spread of these types of malware agents always requires user interaction or, in the case of distribution via Bluetooth, because the range is limited or, last but not least, because there is a shortage of promising eCrime business models. After all, online crime is a profession operated according to the rules of the market economy.



2. Introduction

The development and distribution of malware is an totally professional business and causes damage reckoned in the billions. Criminals have long stopped acting in individual cyber-crime clusters, preferring to share their work across global networks. Malware authors, spammers and data fences work hand-in-hand and are thus able to cover the entire service spectrum of online criminality.

In this eCrime cycle it is absolutely essential, from a financial perspective, for criminals to produce and spread new malware creations at ever shorter intervals, in order to infect, plunder and interconnect as many computers as possible into the botnet infrastructure, as quickly possible.

The predictions made by G DATA at the end of 2007 have come true in 2008: There has been an explosion in the number of new malware agents! In the first six months of this year alone, more than 318,000 new malware agents have been spread - 2.4 times more than in all of 2007.

Malware is spread primarily via websites filled of tools for delivering drive-by downloads. By last year e-mail attachments had already lost their leading position as carriers of malicious files; these days they are used predominantly for luring victims to primed Internet sites. Most new infections now occur through websites. The Internet has thus become a war zone with large-scale minefields!

3. Important events and developments in the first half of 2008

The activities of online criminals surged ahead at full speed in the first six months of 2008. For example, the so-called Storm Worm – already pronounced dead by many at the end of 2007 – celebrated a special birthday.

The Storm Worm gang has split the botnets in such a way that computers behind a router send nothing but spam. Computers with no router are used to host spam and phishing sites. Resolution of a domain name constantly refers to other botnet computers (fast flux). This makes it significantly harder to take malicious websites offline.

More and more malicious code is distributed via compromised websites. Special toolkits make it easier for online criminals to store malware on websites. And then an old technology was revived: boot sector viruses no longer contain file infectors but hidden rootkits these days.

3.1 The "Storm Worm"¹ is celebrating its birthday

The operators of the Storm botnet have proven the power of their zombie armies impressively in the first half of the year. At the same time, the perpetrators use international public holidays and commemoration days for free rides. The criminals had already started Valentines Day (February 14) in mid January but that did not dampen success. The Storm gang's assortment also included "funny" postcards and websites for April 1st. Across the world, a large number of computers were infected and turned into zombies.

After a relatively quiet phase in the last quarter of 2007, Storm is now active again and will probably remain so!



Your download will start in 5 seconds.
If your download does not start, [click here](#) and then press "Run".

Your download will start in 5 seconds.
If your download does not start, [click here](#)

Your download should begin shortly. If your download does not start in 10-20 seconds, you can [click here](#) to launch the download and then press Run. **Enjoy!**

(1) The Storm Worm is technically a Trojan horse but the resulting term "Storm Trojan" is less appealing and also not completely correct.

Background information about the Storm botnet:

In January 2007, storm Kyrill passed over large parts of Europe and caused enormous damage. As soon as the storm had abated, e-mails were circulated promising to provide additional information about the consequences of the storm in the readmore.exe attachment. That is how the Storm Worm got its name (irrespective of the fact that it is not a worm but a Trojan horse and from the same group that had already distributed mails with Holiday and New Year's greetings at the end of December 2006).

The aim of the e-mails is still to integrate infected computers into a botnet that is used for sending spam and for distributed denial of service (DDoS) attacks. Additional waves of email containing false reports („Saddam Hussein alive!“ or „Fidel Castro dead“) and virus warnings followed over the next few months. These emails also contained malicious code as a file attachment.

In June 2007, a change of tactics took place: E-cards and greetings cards lured users to websites where a (malicious) file has to be installed in order to view the card. At the same time an attempt is made in the background to use security holes in the browser or browser components. The infection is then delivered while the greeting card is being viewed. Additional tactics involved downloading codecs for watching videos or software for secure data transfer or privacy protection. Recruiting beta testers was another tactic used.

In September last year, current events were again used to lure victims to malicious websites. It began on Labor Day followed by the start of the new NFL football season. In this case dangerous downloads were marketed as „Free NFL Game trackers“. Additional tactics involved online games, „Krackin“ software, Halloween, and Christmas and New Year's greetings again.

In autumn, the Storm botnet lay low for a while. It appears that the criminals have moved their activities from St. Petersburg to China and Turkey in order to act with even more force.

3.2 Rootkits in the boot sector

As soon as you turn on a computer, the race between malware and security software starts. The earlier control of the system is gained, the better security software can protect the computer or, vice versa, malware can evade protective measures.

Old tactics raked up

At the start of January, malicious code appeared in the wild in the form of Backdoor.Win32.Sinowal. It overwrites the MBR in order to embed camouflage functions in the Windows XP kernel. This new camouflage technology is used to hide theft functions for online banking. In the first half of 2008, 97 variants of this malware occurred. However, the channelling of malicious code into the boot sector is a separate module and independent of the malicious function. It could soon be integrated into other malware as well. This is usually quite an easy task for malware since standard users are able to overwrite the MBR using XP. It is somewhat more difficult with Vista. However, there are protection mechanisms as well: the BIOS often offers the option to write-protect the MBR. Now might be a good time to do so. Earlier boot sector virus vintages were detected by booting from a clean disk.

The G DATA virus solutions' boot CD can reliably detect current MBR rootkits.

According to estimates by G DATA Security Labs it is only a matter of time until additional malware will use this technology for camouflage.

Functionality

The first place in the boot process where control is handed over to changeable software is the Master Boot Record (MBR) of a hard drive or the boot sector of other boot media (e.g. floppy discs). The MBR is the first sector of a hard drive. This is where, amongst other things, the boot loader and partition table of the hard drive are located. The boot loader contains executable code, determines the boot partition and loads the important parts of the operating system (e.g. kernel).

Because the boot sector is the first point at which external code can be channelled into a system, the first viruses such as Brain, Stoned and Michelangelo were boot sector viruses. Hence using malicious code to overwrite the boot sector and take over control as early as possible is not a new phenomenon at all.

Unfortunately, overwriting the MBR is still possible under Windows XP. But hardly any malware has made use of this over the last few years. In 2005, Derek Soeder of eEye Digital Security brought out BootRoot, and with it the possibility that a rootkit can be activated in the MBR. The camouflage functions then become active even before the operating system is loaded. In 2007, Nitin and Vipin Kumar of NVLabs published the VBootkit with which camouflage functions for Vista were implemented. Both BootRoot and VBootkit were technical feasibility studies with no actual malicious function. They have never occurred in combination with malware. But with Sinowal, this has now changed.

3.3 Minefield Internet: click – infect – rob

The threat from infected and primed websites has gathered significant momentum in the first half of 2008, with the effect that the Internet now resembles a war zone. Currently more than 70 percent of all malicious code infections are caused by responding to Internet offers. A further increase is to be expected - especially with the occurrence of sporting events such as the Beijing Olympics. Poorly maintained or hacked fan portals could provide the ideal platform for criminals.

This is how online gangs operate:

Only a very small proportion of e-mails used to spread current malware still contain file attachments. Most of them either link directly to a malicious file or offer the malicious file as a download from a website. Deceptive tactics are often used here, for example, latest news, electronic greeting cards, supposed debits or codecs for interesting films etc.

Malicious code that has been channelled into websites tries to use weak points in the browser or in browser components (such as Adobe Reader or Flash) to silently hijack the computer when the website is called up. Contrary to the assumptions of many users, these **drive-by downloads** very rarely lurk in the red-light districts of the Internet.

Most of the infections originate from normal, popular websites. In doing so, online ads are abused or actual web servers are hacked. This can happen, for example, through weak or stolen FTP passwords or by utilising security holes in popular web applications such as content management systems or bulletin boards.



Forum software as a gateway

In the first third of 2008, an increased number of mass attacks on weak points in web applications have occurred. For example, errors in the forum software phpBB have been responsible for thousands of website contaminations since February. In April, hundreds of websites were attacked using SQL Injection and delivered a malicious IFRAME to visitors of the website. The number of flash-based malware agents has also increased significantly.

For the servers that have thus been taken over, even better tools have been published with which malicious code can be stored on a hijacked website, which is then silently foisted onto the visitor when he or she visits the site.

FirePack, which is now even available in a Chinese version, appeared at the start of the year. In February, a new multi-exploit toolkit appeared. However MPack, IcePack, TrafficPro, Nuclear Malware Kit, Web-Attacker, SmartPack and many others are also traded on the Internet for prices ranging from \$40 to \$3000.

It is clear that malicious code can lurk on any website. Hence, virus protection should be set up so that it checks the HTTP data stream before the browser processes it.

To test this, try to download the text version of the EICAR test file. This is a DOS program that outputs the text „EICAR-STANDARD-ANTIVIRUS-TEST-FILE!“. This is a harmless program that is detected as malware by all anti-virus software.

After downloading the text version of this file from <http://www.eicar.org/download/eicar.com.txt> you will either get a warning message preventing access to the site or the browser will show a line with cryptic text (incl. the above text output). In the latter case, your computer is not fully protected against attacks from the Internet. Script code can be loaded into the browser in the same way as this text. This is executed first and it is only when the browser saves the files as „Temporary Internet Files“ that the virus protection notices that malware has been active; the warning appears but it is too late.

4. Numbers and trends for malware in the first half of 2008

The amount of new malware has again increased significantly; runtime packers share a significant part of the responsibility for this. Botnets, spyware and adware still dominate the scene. The proportion of spam has plateaued at a high level and spammers have come up with a few new tricks. This is detailed in the following sections.

4.1 Malware deluge 2008

2008 could already deserve a chapter in malware history. In ways never seen before, criminals have managed to eclipse 2007 - itself a record year - in the first three months. By the end of March 2008, the G DATA Security Labs experts had already registered more malicious code than in the entire preceding year.

By the end of the year, G DATA expects the amount of new malware to quadruple. The reason for this is that signature scanners only detect known malware. Malware writers exploit this. Malicious code is - as described under "Malware Recycling" in the last malware report - reshaped using packers and other camouflage tools so that the virus signatures no longer apply. This does not affect the functionality of the malicious code itself. Thus changed and now no longer detectable, the code is immediately released.

Another mechanism that leads to the creation of numerous new versions is often used with backdoors. Most backdoors have an update function. This is used extensively as a camouflage mechanism. Backdoors are updated with such frequency that the virus scanner always checks a variant that it does not yet know, because this also means in turn that the new version will not be detected by the signature scanner.

The response time between a virus outbreak and the provision of the corresponding signatures is crucial here.

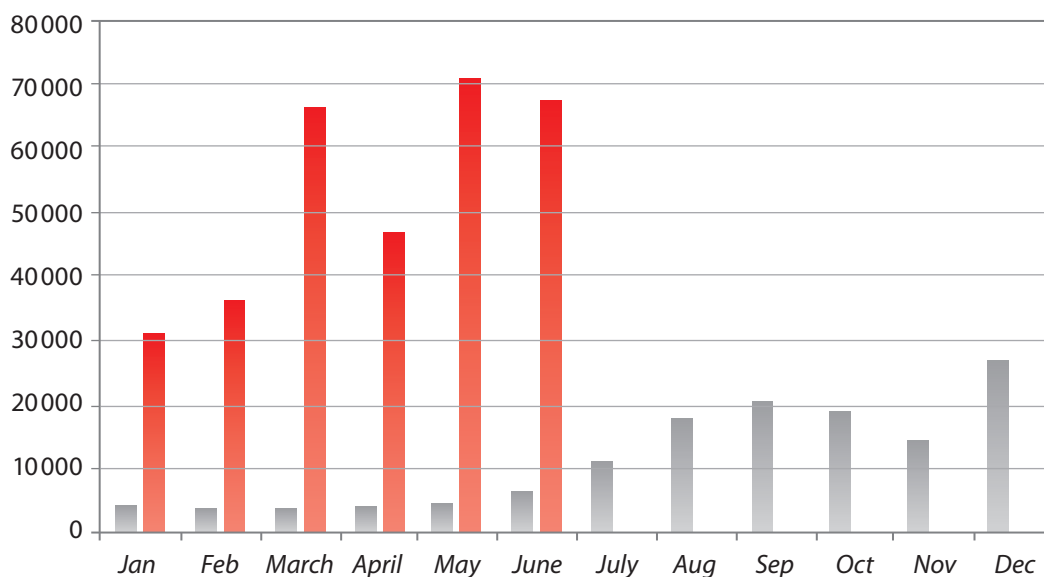


Diagram 1: Comparison - total number of new malware agents ■ in 2007 against ■ the first 6 months of 2008.

4.2 Smartphone viruses: marketing or a genuine risk?

In the first half of this year, G DATA Security Labs were still unable to detect the much-vaunted risk to smartphone owners. Almost all of the 41 new malware agents for smartphones were mere proof-of-concept studies used to test technical possibilities or semi-legal monitoring software for concerned parents or jealous spouses.

The stagnation of this malware type over a number of years comes as no surprise: Its distribution is flawed partly due to the limited range of Bluetooth, partly to the insufficient number of reachable MMS-enabled smartphones and, last but not least, to the fact that both establishing the connection and the installation have to be confirmed by the user.

But the decisive and frequently overlooked reason for this is financial: online crime is big business and therefore subject to the laws of the market. The most important goal is to make as much profit as possible as easily as possible. Smartphone malware is expensive (and not just financially) for criminals to develop. A return on investment has not so far been realistic for the malware industry. Up to now it has been easier to achieve more with less effort in other areas.

So, on the one hand, no profitable business models are available and, on the other, every method of making money currently bears the risk of getting caught. This frequently publicised danger therefore appears to be founded on the politics of marketing and does not have any basis at this point in time.

Month	Number
January 2008	6
February 2008	2
March 2008	9
April 2008	1
May 2008	15
June 2008	8

Table 2: number of new smartphone malware agents

4.3 Botnets and spyware at the top

The distribution of malware according to type is illustrated in table 3. In every category - except for standard viruses - the number of new variants in the first half of 2008 already exceeds the total number for 2007. With a share of almost a quarter, backdoors retain the malware top spot, even though their proportion has dropped significantly since 2007. They form the basis of botnets, which still represent the most effective instruments for online criminals. Downloaders and droppers make up about one fifth of new malware agents.

Criminals use these malware families to install backdoors and other malware on computers. With a share of more than 20 percent, they took second place in new malware for the first six months. Spyware's share has shrunk significantly but it managed to retain third place.

	# 2008 T1	Share	# 2007	Share 2007	Difference
Backdoors	75.027	23,6 %	41.477	31,0 %	362 %
Downloader/ Dropper	64.482	20,3 %	28.060	21,0 %	460 %
Spyware	58.872	18,5 %	29.887	22,4 %	394 %
Trojan horses	52.087	16,4 %	13.787	10,3 %	756 %
Adware	32.068	10,1 %	7.654	5,7 %	838 %
Tools	12.203	3,8 %	1.731	1,3 %	1.410 %
Worms	10.227	3,2 %	4.647	3,5 %	440 %
Dialer	4.760	1,5 %		n.a.	
Exploit	1.613	0,5 %		n.a.	
Rootkits	1.425	0,4 %	559	0,4 %	510 %
Virusses	327	0,1%	2.127	1,6 %	31 %
Miscellaneous	5.170	1,6 %	3.688	2,8 %	280 %
Total	318.261	100,0 %	133.617	100	476 %

Table 3: Number and proportion of new malware types in the first half of 2008 and 2007 and change compared to 2007

4.4 Adware - explosive growth

The amount of new adware had already increased five-fold in 2007. Now it has increased significantly again. Compared to the yearly average for 2007, eight times more malware was detected at the start of 2008. Apart from the tools, this is the biggest increase. Hijacked homepages and files with potentially undesirable content such as adware or manipulated search results are enjoying continued popularity in the eCrime business.

The most common member of this species is Virtumonde. The malware integrates itself into Internet Explorer as a browser helper object and then displays ads in pop-up windows. The multitude of clicks artificially generated in this way fills the adware writers' coffers.



Adware: WinFixer disguises itself as an anti-virus program. Once installed, it hijacks the browser's homepage and constantly displays pop-up ads.

Another type of remuneration is based on the installation of software. Amounts of a few cents are paid for every installation. Again, it is the volume that matters here. The significant increase of new malware shows that this business is profitable.

4.5 Spam on the rise again

In January, the proportion of spam shrank to about 60 percent but then stabilised at about 70%. Since March, the proportion of spam email has been above 80% again, with a top value of 94% in April and 87% at the end of June 2008.

The most common subjects are categorised in the following table:

Subject	
Sexual performance improvement	30 %
Medication	22 %
Replicas	21 %
Academic titles	5 %
Software	3 %

Table 3: Top five subjects of spam email in the first half of 2008

Most spam email is still sent using botnets. In the first half of 2008, it was 85% on average. Every day, between 5 and 10 million zombies are involved in sending spam. Every day, between 200,000 and 500,000 computers (360,000 on average) are turned into new zombies. Most of these are in Germany, Italy and Brazil (see table 4). Hence about 130 billion spam, phishing or malware emails are sent every day.

Land	Percentage share
Brasil	10,2%
Germany	9,3%
Italy	8,9%
Turkey	8,3 %
China	6,6 %

Table 4: Top five countries with the most zombie PCs

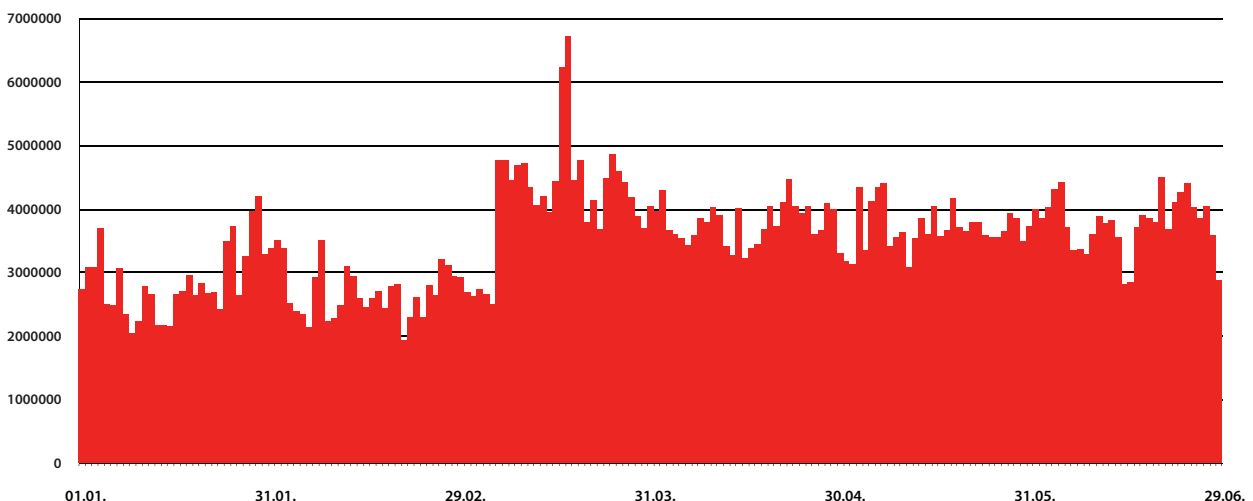
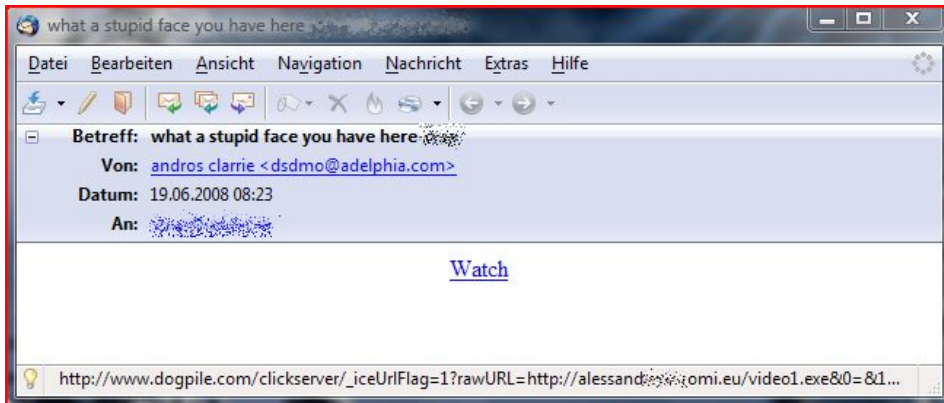


Diagram 2: Spam email in the first half of 2008

To trick spam filters, spammers use known and trusted sites. To do so they use e.g. the redirect functions of Google, Yahoo and other pages. Users and spam filters are thus made to believe that a trusted site is being called up.



A similar approach is also used for images and websites. They are hosted on all sorts of portals such as Flickr or Blogspot. Reputation-based recognition technologies are thus outsmarted.



Diagram 3: images and spam hosted by Flickr and Blogspot

4.6 Online gamers targeted

Looking at the most active virus families in table 5, the Hupigon and Bifrose backdoors are not the only ones that stand out. The old and new front-runner - the Hupigon backdoor - is a member of the malware family that makes the most avid use of runtime packers. New versions can be snapped together quickly and efficiently using a toolkit. Some variants even use 11 different packers.

Trojan horses such as OnlineGames and Magania (GameMania games), which steal access data for online games, have established their place among the most active malware families. This means that online gamers are still being targeted by data thieves. Access data for online games and characters and objects from games are traded for real money in many forums. This also attracts real-life fraudsters.

	#2006	Virus family	#2007	Virus family
1	32.383	Hupigon	16.983	Hupigon
2	19.415	OnLineGames	8.692	OnLineGames
3	13.922	Virtumonde	3.002	Rbot
4	11.933	Magania	2.973	Banker
5	7.370	FenomenGame	2.848	Banload
6	7.151	Buzus	2.627	Zlob
7	6.779	Zlob	2.533	Virtumonde
8	6.247	Cinmus	1.922	Magania
9	6.194	Banload	1.882	LdPinch
10	5.433	Bifrose	1.751	BZub

Table 3: Top 10 most active virus families, 1st half of 2008 and 2007

The other places in table 5 are occupied by the following malware agents:

- **Virtumonde:** adware that integrates itself into IE and displays pop-up advertising.
- **FenomenGame:** misrecognition caused by automatic creation of signatures
- **Buzus:** spy trojan and keylogger with backdoor
- **Zlob:** popular Trojan downloader, which also changes the IE settings to display porn pages and install rogueware.
- **Cinmus** is an adware program, which integrates itself into Internet Explorer and displays pop-up ads.
- **Banload:** downloader for banking trojans, which is mainly aimed at Brazilian and Portuguese banks

4.7 Malware on different platforms - focus on Windows

In the first half of 2008, the proportion of malware for Windows increased from 95.2% to 98.2%. This shows that malware writers are focusing their core business on Windows computers. This is obviously the best place to make money.

	#2008 H1	Platform	#2007	Platform
1	312.668	Win32	126.854	Win32
2	2.650	JS	2.463	JS
3	845	HTML	1.106	HTML
4	572	VBS	1.007	VBS
5	545	BAT	707	BAT
6	252	MSIL	197	PHP
7	231	SWF	166	MSWord
8	92	MSWord	139	Perl
9	91	PHP	137	Linux
10	33	MSExcel	70	ASP

Table 4: Top 10 platforms in the first half of 2008 and whole of 2007

Web-based attacks in JavaScript, HTML, VBScript, Flash (SWF), PHP and Perl have seen their proportion reduce from 2.5% to 1.4%. However, when projected for the whole of 2008, more than twice as many web-based attacks are to be expected. This shows that, apart from Windows malware stored on websites, an increasing number of attacks are executed using web-specific platforms. Since the protection mechanisms for such attacks are yet to mature, they do not have to be updated as often.

Only 21 new malware agents were detected for Linux, and no more than 41 for mobile devices (20 of these were for Symbian, 19 for J2ME and 2 for Win CE in 2007). Hence, the highly publicised danger for mobile phones once again failed to occur in the first six months of 2008.

5. Forecast for the 2nd half of 2008

G DATA expect the following developments in the coming weeks and months:

- **Malware on websites:**
the spread of malware through websites is still far from being exhausted. There are still many gaps to be closed on the surfers' side. It is not just the browser that needs to be firewalled but all its plug-ins as well. There are also quite a few things yet to be done by providers of internet services. Web applications have many security holes such as cross-site scripting, cross-site request forgery and SQL injection, which can be used to channel external content into websites. It will be a while until all web application developers take heed of and implement all necessary security measures. Until then, website visitors will be subject to an increased risk of infection. Only virus protection that also checks HTTP data for malicious code offers reliable protection here. This applies in particular to users who extensively use Web 2.0 offerings such as MySpace, Flickr, Facebook etc.
- **Lucrative business models:**
spam, data theft and adware are billion dollar businesses, which online criminals will not give up easily despite all the law enforcement efforts. Powerful botnets are still the core of this industry. Hence, we will continue to be flooded with downloaders and backdoors that turn computers into spam zombies over the next few months.
- **The trade in data is flourishing.**
These days, spyware sniffs out far more than just online banking access data. Anyone catching a keylogger risks losing his or her entire online identity.
- **Adware is the the fastest growing area.**
A lot of money can be made from fraudulent clicks or the installation of advertising software.
- **New camouflage mechanisms:**
it is possible that rootkits and malicious functions that are integrated into the boot sector or master boot record will be used increasingly over the next few months
- **Bandwagon jumpers:**
upcoming large-scale events such as the Olympics are sure to be used for fraudulent activities.

Go safe. Go safer. **G DATA.**