G Data
Malware Report

Half-year report
January-June 2010

Ralf Benzmüller & Sabrina Berkenkopf
G Data Security Labs

Content

At a Glance

- In the first half of 2010, there were 1,017,208 new malware programs, once again a new record.
- In comparison with the previous half-year, the number increased by 10%, and was a full 50% more than the same period last year.
- In 2010 as a whole, we expect more than 2 million new computer malware programs to be picked up.
- With a 51% increase, spyware is the malware category showing the biggest increase in volume. This is especially true for keyloggers and banking Trojans.
- The volume of new adware has fallen by 40%.
- The two most productive malware families, Genome and Hupigon, resulted in more variants than the entire total of malicious programs in 2007.
- Malicious programs aimed at Windows are the most predominant, representing 99.4% of all occurrences. The proportion of .NET malware, however, climbed by a factor of 3.4 and now represents 0.9%. Even malware authors are taking advantage of the benefits of .NET.
- Malicious code written for Unix derivatives and Java also increased considerably.

Trends

- Data theft is and remains a core function of malware.
- Adware is being superseded by virus protection imitations (fake AV) and blackmailers.
- More and more online services and functions are being misused for malicious purposes.

Events

- Social networks make it into the events lists with plenty of innovations but also a few data leaks. Far in the lead are Twitter and the market leader, Facebook.
- The Mariposa botnet has been put out of action. Spanish police have arrested the three operators.
- The Waledac Botnet, one of the ten largest in USA, has also been hit hard by investigators and 277 .com domains have been removed from the net.
- The German Emissions Trading Authority is the victim of a phishing attack in which the criminals steal and trade permits worth around three million euros.
- PDF files increasingly become the focus of malware authors and consequently reports of weak points in PDF readers abound.

Malware: Facts and Figures

Malware cornucopia

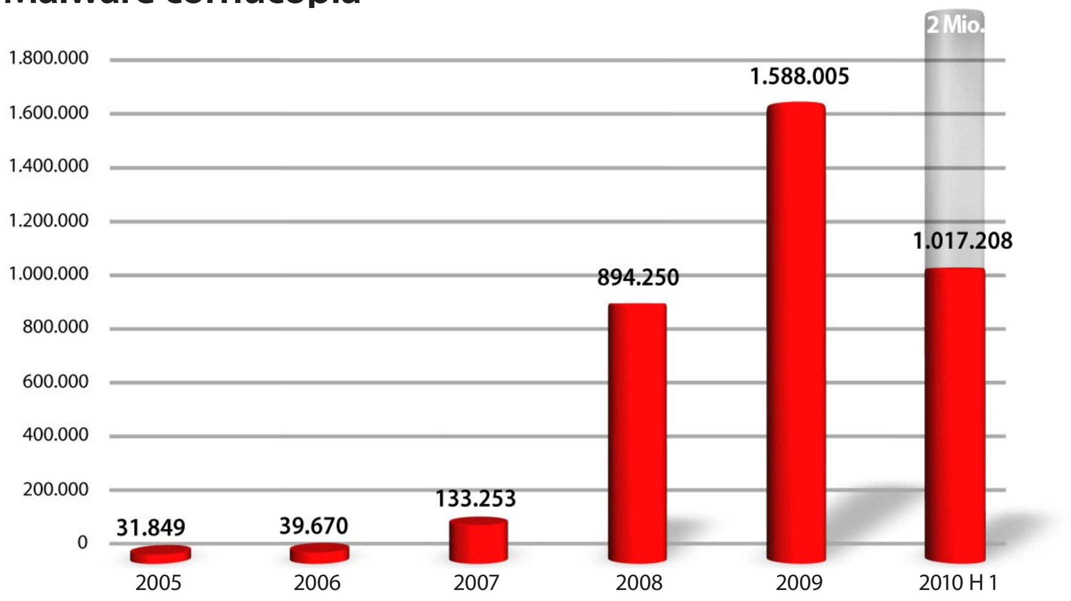


Diagram 1: Number of new malware programs per year since 2005 and in first half of 2010

The 1,017,208 new malicious computer programs[1] detected in the first half of 2010 represented a new record, exceeding the previous half year by around 10%. In comparison with the same period last year, the number was up by more than 50%. In the first half of 2010 alone, more new malicious programs have surfaced than in the whole of 2008. By the end of the year, the number of new malicious programs is likely to break through the two million level.

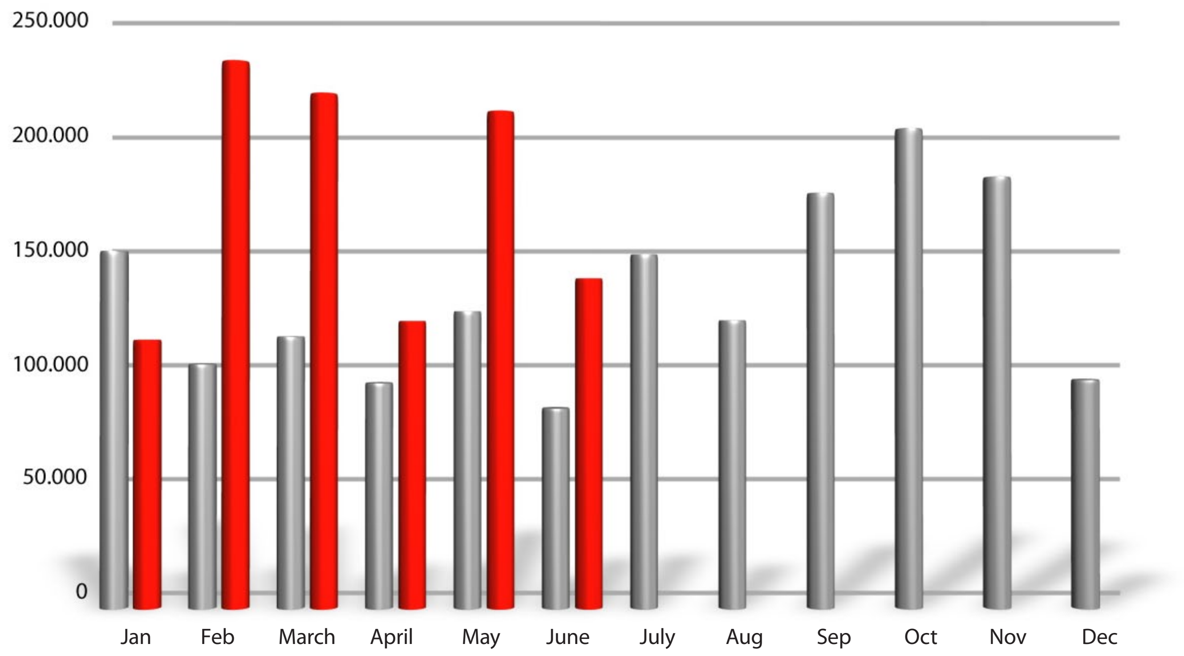


Diagram 2: Number of new malware programs per month for ▨ 2009 and 🟥 2010

[1] The figures in this report are based on the identification of malware using virus signatures. They are based on similarities in the code in the harmful files. Many malicious codes are similar and are gathered together in categories, in which small deviations are referred as variants. Fundamentally different files form the foundation for their own families. The count is based on new signature variants created in the first half of 2010.

Malware categories

The proportion of **spyware** has grown by about 3.4% in comparison with the second half of 2009 - a bigger increase in share than for any other category. Consequently, the considerable downturn recorded in the last G Data malware report has come to an end, even though the share achieved in the same period last year was not reached. In absolute figures this corresponds to an increase of 51%. Particularly high growth rates were recorded in the keylogger[2] and banking trojan[3] **spyware** categories.

In contrast, the increasing use of **rootkits** has continued unabated. Their number again grew over the last half by a factor of 2.6. On the other hand, worms - the meteoric risers of the last G Data malware report - could not sustain that rate of increase, but did however maintain the same level.

The share of **Trojan horses** exceeded the high level of the previous half year. In this group, the level of ransomware (blackmailers and some fake AVs) increased by a factor of 10 in comparison with the same period last year!

The share of new backdoors has fallen by around 2.9% and in so doing is continuing the downwards trend from the first half of 2009. Also the number of **tools** decreased by a factor of about a third, their share falling to 1.0%. The most marked fall was in the quantity of **adware**. In contrast with the previous year (H1 2009 to H1 2010), numbers have fallen by around 40%, with the share falling from 5.3% to 2.1%.

Category	# 2010 H1	Share	# 2009 H2	Share	Diff. 2010 H1 2009 H2	# 2009 H1	Share	Diff. 2010 H1 2009 H1
Trojan horses	433,367	42.6 %	393,421	42.6 %	+10 %	221,610	33.6 %	+96 %
Downloaders/ droppers	206,298	20.3 %	187,958	20.3 %	+10 %	147,942	22.1 %	+39 %
Spyware	130,175	12.8 %	86,410	9.4 %	+51 %	97,011	14.6 %	+34 %
Backdoors	122,469	12.0 %	137,484	14.9 %	-11 %	104,224	15.7 %	+18 %
Worms	53,609	5.3 %	51,965	5.6 %	+3 %	26,542	4.0 %	+102 %
Rootkits	31,160	3.1 %	11,720	1.3 %	+166 %	12,229	1.9 %	+155 %
Adware	21,035	2.1 %	30,572	3.3 %	-31 %	34,813	5.3 %	-40 %
Tools	9,849	1.0 %	14,516	1.6 %	-32 %	11,413	1.6 %	-14 %
Exploits	2,495	0.2 %	3,412	0.4 %	-27 %	2,279	0.3 %	+9 %
Miscellaneous	6,751	0.7 %	5,543	0.5 %	+22 %	4,593	0.7 %	+47 %
Total	**1,017,208**	**100.0 %**	**924,053**	**100.0 %**	**+10 %**	**663,952**	**100.0 %**	**+53 %**

Table 1: Number and share of new malware categories in 2009 and 2010 and their change

[2] 2.5 times compared to the second half of 2009
[3] 2.2 times compared to the first half of 2009

Malware families

Malicious programs can be grouped into families according to their functions and properties. For some of these families, new variants are constantly being produced. While the share of new malicious programs grew constantly in the past, the number of different families reduced. This trend came to an end in the last half year. In the first half of 2010 there were 2,262 active malware families. This is approximately 3% higher than the value for the last half year and approximately one seventh greater than the first half of 2009.

	# 2010 H1	Virus family	# 2009 H2	Virus family	# 2009 H1	Virus family
1	116,469	Genome	67,249	Genome	34,829	Monder
2	32,830	Hupigon	38,854	PcClient	26,879	Hupigon
3	30,055	Buzus	37,026	Hupigon	18,576	Genome
4	25,071	Refroso	35,115	Scar	16,719	Buzus
5	24,961	Scar	24,164	Buzus	16,675	OnlineGames
6	21,675	Lipler	20,581	Lipler	13,889	Fraudload
7	19,385	OnlineGames	19,848	Magania	13,104	Bifrose
8	17,542	Palevo	18,645	Refroso	11,106	Inject
9	16,543	Startpage	16,225	Basun	10,312	Magania
10	16,517	Magania	16,271	Sasfis	10,322	Poison

Table 2: Top 10 most active virus families. Number of new variants in 2009 and 2010

Table 2 shows the families that were the most productive in the last year and a half.
The current leader is still **Genome**, the number of variants having grown by around 73% (H2 2009 to H1 2010). On average, therefore, 640 new variants of **Genome** are produced every day. The number of variants in these families during the first half of 2010 was thus only just lower than the total number of malicious programs in 2007 (see table 1). The second placed family in the last half year, **PcClient** did not make it into the top 10. Old favourites are jockeying for position amongst the other places (see abstract). **OnlineGames** once again made it into the top 10. The **Palevo** worm and **Startpage** browser hijacker families made it into the top 10 for the first time.

Genome

Trojan horses in the "Genome" family combine functionalities such as downloaders, keyloggers and file encryption.

Hupigon

Hupigon functionality includes a backdoor allowing an attacker to remotely gain control of a computer, record keyboard entries, access the file system and switch on the webcam.

Buzus

Trojan horses in the Buzus family scan their victims' infected systems for personal data (credit cards, online banking, email and FTP access details), which are then transferred to the attacker. Furthermore, the malware attempts to lower the computer's security settings so that the victim's computer can be more easily attacked.

Refroso

This Trojan horse surfaced for the first time at the end of June 2009. It has backdoor functions and can attack other computers in a network.

Scar

This Trojan horse loads a text file which is used to initiate further downloads of malware such as downloaders, spyware, bots etc.

Lipler

"Lipler" refers to a downloader family that can download additional malware from a website.
It also changes the browser's start page.

OnlineGames

Members of the OnlineGames family primarily steal online games login data. To do this, various files and registry entries are searched and/or a keylogger is installed. In the last case, it is not only games data that is stolen. Most attacks target games that are popular in Asia.

Palevo

The "Palevo" worm spreads via removable media (autorun.inf), copying itself under tempting names in releases of peer-to-peer file sharing programs such as Bearshare, Kazaa, Shareaza etc.
It also distributes links to harmful websites via instant messaging (primarily MSN). It injects backdoor functions into Explorer and searches for commands on particular servers.

Startpage

This malware family changes the start page and often many other browser settings as well.
It represents the most prominent variant of the browser hijacker.

Magania

Trojan horses in the Chinese Magania family specialise in the theft of gaming account data from Taiwanese software producer, Gamania. In general, copies of Magania are distributed via an email that contains a multiply-zipped, nested RAR archive. When executing the malware, an image is first displayed as a distraction while further files are loaded onto the system in the background.
In addition Magania inserts itself in Internet Explorer so that it can read the web traffic.

Platforms: .Net increasing

As before, the majority of malware is written for Windows. The proportion of executable files amongst Windows (Win32) malware has fallen to 98.5%, although the actual number has increased by around 9%. Consequently a trend is continuing that we reported on in the last malware report. However, once again the lower number of Windows malware programs is compensated for by the increase in malware written for the .NET platform by a factor of 3.4. Even malware authors are taking advantage of the benefits of .NET, especially because it is supplied as standard in recent operating systems. In total, the share of Windows malware programs is thus about 99.4%.

Of the remaining 0.6%, website malicious code (e.g. JavaScript, PHP, HTML, ASP etc.) accounts for approximately two thirds (i.e. 0.4%). This area has recorded a slight decrease in the number of new variants. However, the existing variants are very prevalent.

	Platform	# 2010 H1	Share	# 2009 H2	Share	Diff. 2010 H1 2009 H2	# 2009 H1	Share	Diff. 2010 H1 2009 H1
1	Win32	1,001,902	98.5 %	915,197	99.0 %	+9 %	659,009	99.3 %	+52 %
2	MSIL[4]	9,383	0.9 %	2,732	0.3 %	+243 %	365	0.1 %	+2471 %
3	WebScripts	3,942	0.4 %	4,371	0.5 %	-10 %	3,301	0.5 %	+19 %
4	Scripts[5]	922	0.1 %	1,124	0.1 %	-18 %	924	0.1 %	-0 %
5	NSIS[6]	260	0.0 %	229	0.0 %	+14 %	48	0.0 %	+442 %
6	*ix[7]	226	0.0 %	37	0.0 %	+511 %	66	0.0 %	+242 %
7	Java	225	0.0 %	31	0.0 %	+626 %	3	0.0 %	+7400 %
8	Mobile	212	0.0 %	120	0.0 %	+77 %	106	0.0 %	+100 %

Table 3: Top 5 platforms in 2009 and 2010.

Malware on other platforms is disappearing from this mass. Despite this, it is worth noting that the number of malware programs for Unix-based operating systems has increased by more than a factor of six, while malware for Java has increased by a factor of seven (each relative to the second half of 2009).

[4] MSIL is the intermediate format in which .NET applications present themselves in platform- and programming language-independent form.

[5] "Scripts" are batch or shell scripts or programs that have been written in the VBS, Perl, Python or Ruby scripting languages.

[6] NSIS is the installation platform that is used for installing the Winamp media player etc.

[7] *ix stands for all Unix derivatives, e.g. Linux, FreeBSD, Solaris etc.

Conclusion and trends 2010

The flood of malware is not abating. Backdoors, rootkits, spyware and the like each have a firm place in a flourishing underground economy. Malware authors are paying particular attention to spyware in the keylogging, online banking and online games areas. Data theft is and remains one of the core functions of malware. Marketing this is a firmly established practice in underground forums.

The number of new adware variants is falling significantly. This is possibly related to the fact, that with more aggressive "advertising methods", imitation antivirus programs (fake AV) or encryption and protection software (ransomware), can earn more money.

Windows remains the most important target of attack. However the malware authors are increasingly searching for alternatives.

Outlook

Category	Trend
Trojan horses	→
Backdoors	→
Downloaders/droppers	→
Spyware	→
Adware	↘
Viruses/worms	→
Tools	→
Rootkits	↗
Exploits	↘
Win32	↘
WebScripts	↗
MSIL	↗
Mobile	↗
*ix	↗

Events during the first half of 2010

January 2010

04.01. **Strange but true**: The website of the Spanish **EU Council Presidency** presents a new face, in the truest sense of the word when a **hacker** uses a cross-site scripting attack to replace the portrait of Spanish Prime Minister Zapatero with an image of the fictitious comedy character Mr. Bean.

06.01. **Strange but true:** A 26-year old Britain vents his spleen on **Twitter** and a week later is **arrested** for doing so! "You‘ve got a week and a bit to get your s*** together, otherwise I‘m blowing the airport sky high", was his "threat" to the Robin Hood Airport in Britain, because he feared that his flight on January 15th could be cancelled due to the bad weather. He was held for almost seven hours for this Tweet, lost his job and received a lifelong exclusion order from Doncaster Airport. The Internet community affectionately baptised Paul Chamber a "**Twidiot**". Chambers himself cannot understand the fuss.

12.01. The "**Iranian Cyber Army**" seize the largest Chinese search engine **Baidu** using modified DNS entries and leave behind a confession banner. In December 2009, they also crippled the Twitter micro-blogging service for for several hours, again using modified DNS entries.

14.01. The operators of website **opendownload.de** lose a case on appeal in the Mannheim County Court, without any chance of a further appeal. At the start of 2008 a user was sent a **bill** from opendownload.de, although a duty of payment was not "easily identifiable and sufficiently perceivable to ensure that the average consumer would be informed of the resulting costs without further information," according to the **Mannheim County Court** in its ruling. Via his lawyer, the customer refused payment and moreover claimed for his legal fees. The Rheinland-Palatinate consumer advice centre had already issued a report on the questionable methods employed by the website at the end of 2008.

14.01. A former administrator of **underground website DarkMarket** was sentenced to 10 years imprisonment. The 33-year old man from London, Renukanth Subramaniam, had unknowingly been running the website alongside an **FBI** agent working undercover. The American feds set up the website and used it to carry out investigations into cyber-criminal circles.

19.01. In the blog on the website **netzpolitik.org**, it is reported that the company Ruf-Jugendreisen has had data stolen in a **Cyber attack**. The attackers got hold of data concerning the tour operator's mainly young community members. According to netzpolitik.org, Ruf had apparently been tipped off three years ago about **security holes**, but apparently ignored them, it was stated on January 21st.

21.01. **Microsoft** publishes a **security patch** outside the normal cycle. The emergency patch was urgently required, because the **Exploit** code, which enabled attacks in December 2009 on Google and other companies, was published on the Internet at the start of the week. In total the patch resolves eight security holes.

Illustration: G Data 2009

25.01. The **Cyber attacks on Google** and other companies, which at the start of January had considerable repercussions, were only possible through **social networking** sites. Experts have discovered that the attackers located persons in key positions, spied on them using Web 2.0, then compromised accounts belonging to friends of the victims. Camouflaged as friends, they sent messages with links to infected websites and thus got access to corporate networks. The group considered withdrawing from **China's** economy and closing google.cn.

29.01. The **German Emissions Trading Authority** (DEHSt) comments on **phishing attacks** carried out on the previous day: Scamsters circulated their fraudulent emails as email from the DEHSt and persuaded the recipients to login to a counterfeit website, ironically to protect themselves against alleged hacker attacks. Using the stolen access data, the attackers transferred emissions permits, primarily to Denmark and Great Britain, and in so doing allegedly got away with up to three million euros. It is readily apparent that targeted phishing attacks can be very lucrative.

February 2010

02.02. **Twitter passwords** reset: Managers at the microblogging service Twitter recorded attacks on their users, which most probably have been carried out with the aid of torrent pages; most affected are users who have used **the same login data** on several platforms and were therefore open to attack. Passwords should be different for every account. Simple variations to a base password are often sufficient.

03.02. The websites of popular German **online news portals** have fallen victim to so-called **malvertising**. Golem.de, Handelsblatt.com and even Zeit.de temporarily delivered malware to the visitors of their web pages via infected advertising banners. The danger of an infection is no longer limited to the seedier sites of the Internet. Reliable virus protection must check the contents of web pages for malware.

03.02. Edwin Andrew Pena pleaded guilty before a New Jersey District Court to earning around US$ 1,000,000 between 2004 and 2006 through the **illegal sale of voice over IP minutes**. Pena routed the data packets via servers of telecommunications service providers who only "protected" their servers with the preset **default passwords**.

09.02. Five days after the message about two infected **add-ons**, **Mozilla** has to admit that one of the two add-ons was incorrectly detected. A subsequent scan recognised the apparently infected tool as a **false positive**.

09.02. A tool for removing a Trojan horse from a computer replaces it with something else instead: „**Kill Zeus**" is the name of the "Spy Eye Toolkit" program - which does indeed remove the "Zeus Trojan" from a computer, but which has dishonest intentions itself and in turn reads user data and passwords. The **Zeus-Toolkit** has been circulating since the end of 2009 in underground forums and sells for around US$ 500.

09.02. A **Dutch scareware** program surfaces on the net. Even though the user interface is full of spelling errors, the existence of a non-English version is seen as an unmistakable expansion to non English-speaking countries. In total this scareware program supports **19 languages**.

10.02. The **Australian government** is crippled by the targeted **DDoS attacks** by the "Anonymous" activist group. The attacks are labelled as politically motivated hacktivism and strongly condemned both on the government website as well as by opponents of censorship. Reason for the excitement: Australia plans the **censorship** of selected online pornographic content, so that censorship opponents fear unreasonable filtering.

17.02. **Strange but true**: A group of young **Dutch people** publish the website **PleaseRobMe.com**, to highlight the danger of improvident absence messages on social networks. We should be aware that our tweets and posts about our **location** are available for all to read and generally not just for friends. Consequently thieves know when someone is definitely not at home and can use the circumstances to their advantage. According to hearsay, insurance companies are considering an increase in insurance premiums, if customers demonstrably use such services to give away their **geographical location**.

17.02. **Microsoft** explains that the **Alureon rootkit** is responsible for the **bluescreen** crashes of many Windows XP and a few Windows 7 computers. The Bluescreens of Death (BSoD) became more frequent after the MS10-015 system update the previous week. The machines affected were infected with Alureon prior to the update.

PLEASE ROB ME

Listing all those empty homes out there

Check out the same results on Twitter search.

Screenshot 1: Source: pleaserobme.com

23.02. **Microsoft** announces that it has carried out a hard and, until now, unique strike against one of the ten largest botnets in the USA, "**Waledac**". It implemented the legally granted authorisation to remove 277 .com Internet domains from the network, which were believed to have a connection with the "Waledac" botnet. Consequently the infected **bot computers** lose contact with the controlling command & control servers.
The "Waledac" botnet is estimated to have sent more than **1.5 billion spam emails** per day.

Illustration: G Data 2009

March 2010

01.03. It becomes apparent from instances of the so-called "**Operation Aurora**" against Google and well over a hundred other companies that the attacks could well have been orchestrated using **infected PDF files**. On a few of the computers which were investigated by forensics, there were harmful PDF documents, which to all intents and purposes could have been associated with the attack. The files have similarities in terms of time, origin and type to other clues found up until now. Linked to this, chip manufacturer **Intel** announces in its annual report that it was also affected by an "**ingenious security incident**" in January, however the company gives no information about the extent or the effects.

03.03. The Spanish authorities announce that they have arrested **three alleged operators** of the "**Mariposa**" botnet (Spanish; English = butterfly). The Spanish men, aged between 25 and 31, are alleged to have stolen mainly online banking and credit card data using the botnet. According to estimates, the extent of the network is **more than 13 million computers** in 190 countries.

06.03. A large number of **Twitter accounts** were**hacked** and tweeted spam about an apparent diet. "Check out this diet I tried, it works!" and "I lost 20 lbs in 2 weeks" were the enticing calls. Still unconfirmed, but conceivable, the accounts were compromised using **brute force attacks** (dictionary attacks) against Twitter interfaces (APIs).

07.03. A survey by GlobeScan for the BBC World Service reveals that nearly **80% of the population** considers access to the **Internet as a basic right**. Regulations already implemented in countries such as Finland and Estonia are desired by the majority of the 28,000 or so respondents from 26 countries, of whom 14,306 respondents are already Internet users themselves.

09.03. **Twitter** starts a new security measure with regard to sent links. All links sent to Twitter are **checked** for possible malicious effect (phishing and other attacks) before being sent out. This should uncover, intercept and prevent distribution of harmful links via the Twitter service.

10.03. Users of **Internet Explorer 6 and 7** browsers are targeted by hackers. Microsoft publishes a security warning about a **0-day exploit**. Under certain circumstances, attackers could execute harmful commands on the attacked PCs. Internet Explorer 7 is still especially widespread and experts forecast mass exploitation of the security hole following publication of the exploit code.

11.03. The number of command & control servers in the **ZeuS botnet** has again recovered. The Swiss initiative ZeuS Tracker recorded a massive decrease within the past two days of C&C server numbers (from 249 to 104) and has tracked this back to upstream provider Troyak-as being temporarily switched off. The **number of servers** has recovered since then so that it now stands at 191.

12.03. The official annual report of the **Internet Crime Complaint Center** (abbreviated to IC3) records an increase in **complaints**. In 2009 there were 336,655 cases, which is an increase of 22.3% relative to 2008. The lion's share of the notifications were due to Internet fraud in connection with financial loss, which is running at **US$ 559.7 million**. IC3 is an association between the FBI and the National White Collar Crime Center and is the central ombudsman for Internet crime in the USA.

16.03. Two **high school pupils** from Heeswijk-Dinther in the Netherlands were expelled from school, as they had used **keyloggers** to gain access to **19 teacher email accounts**.

They stole examination documents and shared the information with their friends.

19.03. A **critical security hole** in the browser **Firefox 3.6** causes Bürger-CERT (citizen CERT), a project of the German Federal Office for Information Security (BSI), to issue a warning about its use. For the time being users should no longer use version 3.6. Mozilla reacts quickly and on March 23rd releases a security patch closing the **CVE-2010-1028** security hole.

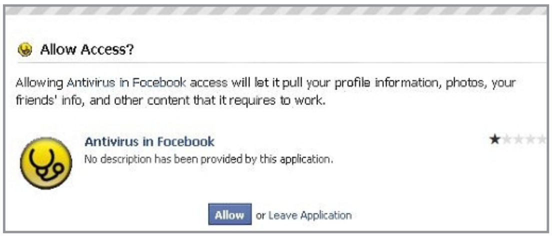
22.03. Mobile network provider Vodafone admits that it has delivered a total of nearly 3,000 units with **infected memory cards**. Three weeks previously, after a malware analyst discovered the malware after purchasing the **smartphone**, Vodafone reported that this was definitely an isolated case. The incident is limited to **Spain**. Supposedly affected customers are contacted and tools for removing the malware are made available. It makes sense to check new gadgets for viruses.

24.03. The organisation **Messaging Anti-Abuse Working Group** (MAAWG) publishes the results of a study about user behaviour relating to the subject of **email security**. The studies carried out in America and Western Europe indicate: 43% of the 3,716 respondents opened email that they themselves classed as **spam**, and 11% even clicked a link in one of these emails. 8% considered it was impossible that they could become the victim of a bot infection.

26.03. In the USA **Albert Gonzalez** was condemned to 20 years imprisonment. The 28 year old man, is effectively the brains behind probably the "biggest and most expensive example of computer hacking in the history of the United States", according to the sentencing judge. Together with two **Russian accomplices**, Gonzales is said to have stolen over **130 million sets of credit card and bank card data records**.

29.03. Security expert **Didier Stevens** uses a **PDF function** to launch any program upon opening a PDF document. In this case, switching off of the Javascript function offers no protection. Until the publication of an update, Foxit Reader executes the code without any further enquiries, Adobe reader displays a warning message. However, the text in the warning window that is triggered can be changed and provides opportunities for **social engineering**.

30.03. A **Facebook** antivirus application spreads within the social network; however it is a scamming attempt, as there are no dedicated protection applications for the market leader. After installation **of the counterfeit app**, it inserts 20 friend labels into an image to entice further friends into the trap.



Allow Access?

Allowing Antivirus in Focebook access will let it pull your profile information, photos, your friends' info, and other content that it requires to work.

Antivirus in Focebook

No description has been provided by this application.

Screenshot 2: "Fake Facebook antivirus"
Source: SecurityWatch Blog

31.03. **Facebook** is in the headlines again: Inadvertently the network giant displayed **all the email addresses** for the 400 million or so users for about 30 minutes **openly** on the profiles. The users had no chance to delete or hide the addresses.

31.03. As is now known, the website of the **German Federal Environmental Agency** distributed a **ZeuS Trojan** between March 19th and 22nd. How the site became infected is not officially known.

April 2010

01.04. A new **expert centre focused on the subject of cyber crime** opens in **Belgium**. The University of Leuven is cooperating in this along with other academic institutions, the Belgian government, the European Commission and a few private companies. The aim of the centre is to develop suitable training measures and to increase awareness.

15.04. After details about a **security hole in Java's development tool kit** were made available to the public two days previously, today sees the Java 0-day exploit "in the wild" for the first time. Tavis Ormandy and Rubén Santamarta publish detailed information about the security hole. Sun quickly decides on an **out-of-cycle update**, however only long after predictions of an **infection wave** have amassed. Version 6u20 is available for download from today and closes the hole.

15.04. A **Japanese malicious computer program** spreads by downloading **counterfeit Hentai computer programs** from P2P networks. It accesses information on infected computers and makes it accessible on a homepage. The information is in the form of reports giving the name of the victim, IE favourites, browser history, etc. The victims receive an email and are requested to make a payment of **1,500 Yen** to have their data deleted from the website.

15.04. The **Dutch railway company**, Nederlandse Spoorwegen, combats **skimmers**. Since August 2009, the company has been changing all the card slots in its automatic ticket machines, after a total of 467 skimming devices were discovered on the machines. So far in 2010 no third-party apparatus has been detected.

Illustration: G Data 2009

16.04. An employee of **Gwent police** (UK) **sent** an explosive Microsoft **Excel table** containing personal data and information from **the police criminal records** of 10,006 people. Due to the "AutoComplete" function being switched on in the email program - and carelessness - the **unencrypted and unsecured** list fell into the hands of a journalist working for "The Register". In cooperation with the Police, the list was deleted from the journalist's system and not published.

19.04. The **Dutch hacker "Woopie“**, 22 year old Kevin de J., is arrested. He is accused of hacking into the CrimeClub and ExtremeClub websites and stealing and publishing **scripts** from the administrator database. Allegedly he had paralysed the sites using **DDoS attacks**. His own website, woopie.nl, was confiscated by the police special unit, Team High Tech Crime. It is probably the first time that a website has been confiscated in the Netherlands.

21.04. From today **Facebook** has introduced a significant change to the **privacy settings**. The function is called "**Instant Personalization**" and allows website providers to access the public profile of users, so that the websites called up can be personalised. The "Instant Personalization" function has been created as a so-called **opt-out**, which means that it applies for every user unless they uncheck the function. This function is another step on the path to the **transparent user** and can be used both for marketing purposes/targeted advertising as well as by **identity thieves** carrying out searches.

22.04. **Strange but true**: In April 2010 nearly **900 .be domains have already been hacked**, according to the statistics from zone-h.org. The web log Belsec mentions that the number of hacks this month is **exceptionally high**. One possible reason under consideration is the use of shared hosting, i.e. managing multiple websites on one web server.

24.04. "**Blippy**", a type of Twitter for online shopping tours. Confirmed **purchases** are displayed on the network as **short messages**, including price details and a description of the purchased articles. However, five members of the web 2.0 service found their **credit card data posted by Google**. According to "Blippy" these were "isolated cases", which originated from the earlier beta testing of the service.

27.04. The **Google Street View** project has once again been the subject of criticism for several days. In its official Google Policy Europe Blog, Google gives details about the data collected by Street View cars. The WLAN (WiFi) data collected by the cars includes SSID and MAC addresses according to the statements. The German Federal Data Protection Commissioner, Peter Schaar, requested the immediate deletion of the data and a stop to future data collection. Google states that it does not collect and store payload data (sent data packets). This information is revised on 14.05.10.

29.04. A **Bulgarian skimmer** is sentenced to **four years imprisonment**, after operating skimming machines in Bruges, Antwerp and Brussels. He was sentenced for breaking of the applicable banking transaction laws and for membership of an international organised **crime organisation**.

May 2010

04.05. Two of the probable heads behind the **Mariposa Botnet**, "Netkairo" and "Ostiator", attempted to gain employment with a Spanish **security software company**. The head of the company said, in connection with the application, "I don't know what they thought, but using Mariposa on their business card is not really a great help, in fact rather the opposite." As the company made it apparent that they weren't interested in making an appointment, one of the two applicants threatened to reveal security holes in their software.

04.05. The Internet portal **netzpolitik.org** once again reports massive data theft from the German Web 2.0 platform for pupils, **SchülerVZ**. Although the operators of the VZ portal have indeed invested in data security since the last incidents and have amongst other things achieved a **TÜV test mark for data security and functionality**, one student was able to collect data on **more than two million**, mainly underage users. His crawler would work equally well with the platforms MeinVZ and StudiVZ; however it was the programmer's intention to draw attention to protecting underage users' data. According to its own data, SchülerVZ had over 5.8 million members in May 2010.

05.05. A fresh **security hole in Facebook** excites a furore: The **preview option** for a user's own profile, located in the private sphere settings, opens unintentional views of the person's live-chats and contact

Screenshot 3
Source: Facebook.com

requests when selected in a preview viewer. Facebook reacted and initially took the chat function off the net.

14.05. Information given at the end of April about the scope of **WLAN data collected by Google Street View cars** proves to be false. In a blog entry written by Alan Eustace, Google admits that "**unintentional samples** of user data from open (e.g. from networks without any password protection) **WiFi networks** were collected". "Moreover, in consideration of the concerns that have arisen, we have decided that the best course of action is to completely cease the collection of WiFi network data by our Google Street View cars."

17.05. Around 200 **soldiers in the Israeli military** apparently had the wool pulled over their eyes by the **Lebanese Shiite Militia** on the Facebook social network. Camouflaged behind the Israeli name Reut Zukerman and a woman's photograph, the manipulators behind the profile are said to have garnered inside information about the armed forces. The armed forces had been warned over a year ago that Internet friendships were risky.

18.05. The Spanish company UPCnet issues extrapolations according to which **Spanish public facilities** are subject to around **5,400 cyber attacks** per year. The measurements were created using the SIGVI program by the Technical University of Catalonia, which records between **12 and 15 attacks** per day on the university alone..

19.05. One of the largest **criminal underground forums** has been hacked: „**Carders.cc**", a platform which is primarily concerned with the subject of credit cards. The purported attackers are supposedly those who, in November 2009, also hacked the "**1337 Crew**" forum. The bounty from the latest hacker attack: a **database containing email addresses, IP addresses and more**.

24.05. Aza Raski, an employee of **Mozilla Labs**, publishes a **proof-of-concept** for "**Tabnabbing**" as he has christened it. With the aid of Java script, the favicon and page content of an open browser tab is changed after it is not viewed for a certain period of time. The changed page can then **impersonate any login page**, making the user think that they themselves called it up. If the user then enters his login data, the **phishing attack** has worked.

June 2010

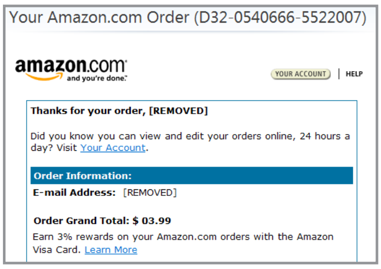
04.06. On its website **Adobe** reports a **critical security hole (CVE-2010-1297)** for Adobe Flash Player 9.0.277.0 and 10.x, Adobe Reader 9 and Acrobat 9 and 8, which extends across different operating systems. Computers are compromised via specially prepared flash files.

07.06. **Japanese police forces** have arrested two men for data theft and blackmail, in association with the spreading of a **malicious computer program** via **Hentai games**. The malicious program collects the victim's personal information from their computer and publishes it on a website. The two are alleged to have worked together since the end of 2009, infecting **at least 5,000** computers and in so doing pocketing over **3.8 million yen** (approx. 34,000 euro).

10.06. On its website Microsoft reports a **security hole in the Microsoft Help and Support Center**, which can be used with some versions of Windows XP and Windows Server 2003 **to**

spread malicious code. Calling up help documents can open the gate for attackers, who then use the security holes to launch programs on the victim's computer or to download malware onto it.

25.06. A wave of **counterfeit Amazon.com** and **Buy.com order confirmations** lands in email boxes. The website linked to contains malware and is currently downloading **fake AV software** onto the victim's computer. The special thing about this **scareware** is that it can read and display stored **passwords** from Internet Explorer 6.



Your Amazon.com Order (D32-0540666-5522007)

Thanks for your order, [REMOVED]

Did you know you can view and edit your orders online, 24 hours a day? Visit Your Account.

Order Information:

E-mail Address: [REMOVED]

Order Grand Total: $ 03.99

Earn 3% rewards on your Amazon.com orders with the Amazon Visa Card. Learn More

Screenshot 4: "Fake Amazon order"

28.06. According to a representative survey by the **German Association for Information Technology, Telecommunications and New Media (BITKOM)**, 41 percent of German citizens do not change their **passwords** for online accounts, email boxes etc. unless prompted. And women are are the worst when it comes changing login data: 45% of them never change it, in contrast to 38% of men. The most common reason for **updating laziness** is supposedly the fear of forgetting the password. This ensures **data thieves** have it easy.