



G Data MalwareReport

Half-yearly report July - December 2010

Ralf Benz Müller & Sabrina Berkenkopf
G Data SecurityLabs

Go safe. Go safer. **G Data.**



Contents

At a Glance	2
Malware: Facts and Figures	3
The end of the growth?	3
Malware categories	4
Malware families	4
Platforms: Windows and Web	6
Trends for 2011	7
Top subjects for the second half of 2010.....	7
WikiLeaks brings 'Hacktivists' into the arena	7
Industrial facilities at risk: the Stuxnet incident	8
Attacks: Java supersedes PDFs.....	9
Events during the second half of 2010	10
July 2010	10
August 2010.....	10
September 2010.....	11
October 2010.....	13
November 2010.....	13
December 2010	15

At a Glance

- In line with expectations the number of new computer malware programs has again increased in 2010, reaching a total of 2,093,444. This marks a rise of 32% over 2009 and is a new record.
- However, the increase slowed down to a single digit percentage range in the second half of 2010.
- Adware is the most increasing (+66%) malware category in the second half of the year, reaching a new high since the first half of 2009. Overall it was in 6th place in the most active categories of 2010. Malware families in the online games sector were not among the Top 10 of most active families in this half-year. These places are quickly being filled by new forms of fraudulent software.

Trends

- Malware authors are focusing more and more on security holes in Java.
- The incidents involving Stuxnet illustrate that security problems are not just limited to desktop and server PCs - industrial facilities are at risk as well.

Events

- Fortunately in 2010 a number of cyber-criminals of influence in the underground were arrested and several botnets were shut down. The investigations made it clear that only international collaboration between authorities can produce such a result, as organised crime in the Internet age is mostly operated on an international level.

Outlook for 2011

When looking into the near-future for 2011, we will probably see the Java platform becoming a very popular target for cyber-criminals in 2011, if not even the top target, as happened with Adobe in 2010. Furthermore we will again see sophisticated botnet activity and potentially even combinations of botnets to avoid possible intervention by law enforcement bodies.

Targeted attacks launched by 'hactivism', cyber-espionage or cyber-sabotage or even a combination of these could become the biggest problem to be expected in 2011, as they start off 'under the radar'. Thus the real problem is almost something else: will we even notice the attacks?

In any case we will observe further exploitation of social networks. Location services and URL abbreviation services will create even bigger malware problems for social networks in the future. The lack of awareness of personal privacy among home users and the wealth of data concerning individuals (including in the cloud) enable cyber-criminals to use specifically-designed malware to launch targeted attacks against every private individual, every business and every organisation in the world.

Malware: Facts and Figures

The end of the growth?

In the second half of 2010 the number¹ of new malware programs increased by 1,076,236. This is 5,849 per day on average. Overall in 2010 over 2 million new variants of malware programs emerged (see figure 1) - 32% more than in 2009 and almost 52 times more than in 2006.

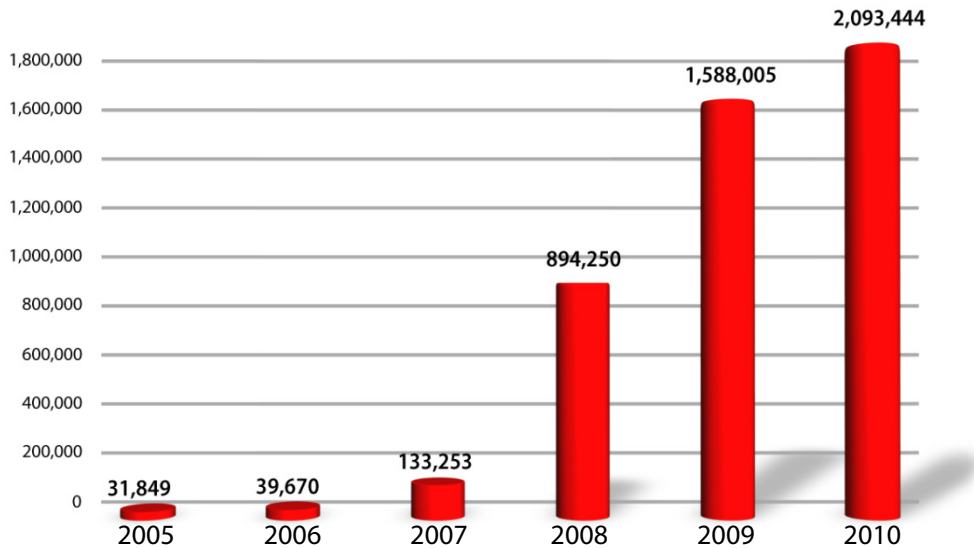


Figure 1: Number of new types of malware per year since 2005

However, when considering the distribution across individual months, it is apparent that the increase has slowed significantly since the second quarter of 2009, i.e. to 16% against the previous year and just 6% more than the first half of 2010. The rate of growth was in the single digit range for the first time in a long time and for now this is not predicted to change.

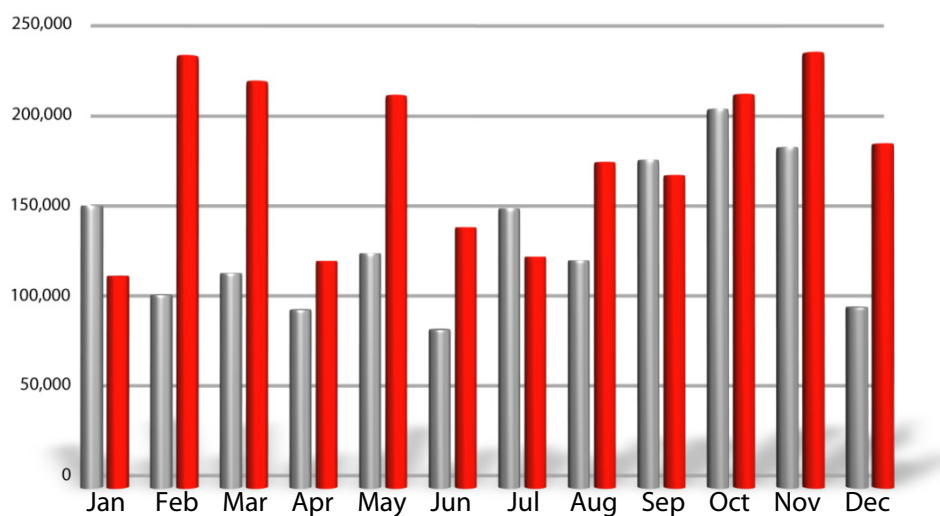


Figure 2: Number of new malware threats per month for 2009 (grey) and 2010 (red)

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

Malware categories

Malware can be subdivided into categories based on its principal malicious activities. In Table 1 the number and proportion of individual categories for the last half-year and the differences between the individual half-years are listed. The majority of new malware variants were in the **Adware** sector. The trade in fraudulent clicks and advertising displays is flourishing. The number of **downloaders** has also increased again at above-average rates. The number of new **backdoors** has also increased significantly over the first half of 2010 again (+22%), compensating for a decline below the level of the second half of 2009 in doing so. The number of new **rootkits** has decreased significantly compared to the first half-year. The large increase in the first half of the year was thus put into perspective. Compared to the previous year the increase corresponds to an average increase of around 5%. However, the number of **exploits** has dropped for the third time in a row.

Category	# 2010 H2	Share	# 2010 H1	Share	Diff. 2010 H2 2010 H1	# 2009 H2	Share	Diff. 2010H2 2009H2
Trojan horses	447,644	41.6%	433,367	42.6%	+3%	393,421	42.6%	+14%
Downloaders/Droppers	240,124	22.3%	206,298	20.3%	+16%	187,958	20.3%	+28%
Backdoors	149,723	13.9%	122,469	12.0%	+22%	137,484	14.9%	+9%
Spyware	113,117	10.5%	130,175	12.8%	-13%	86,410	9.4%	+31%
Worms	48,324	4.5%	53,609	5.3%	-10%	51,965	5.6%	-7%
Adware	34,882	3.2%	21,035	2.1%	+66%	30,572	3.3%	+14%
Tools	13,499	1.3%	9,849	1.0%	+37%	14,516	1.6%	-7%
Rootkits	12,305	1.1%	31,160	3.1%	-61%	11,720	1.3%	+ 5%
Exploits	1,691	0.2%	2,495	0.2%	-32%	3,412	0.4%	-50%
Miscellaneous	14,927	1.4%	6,751	0.7%	+121%	6,595	0.6%	+126%
Total	1,076,236	100%	1,017,208	100%	+6%	924,053	100%	+16%

Table 1: Number and proportion of new malware categories and changes over the past three half-years

Malware families

Malware is grouped into families based on properties and activities. Some families constantly generate new variants. Table 2 shows the most prolific families in the last half-year. Following the concentration of smaller and smaller malware families that has occurred in recent years, the opposite trend was resumed in the first half of the year. The number of active families in the second half of 2010 was 2,608, placing it some 15% above the level of 2,262 in the first half of the year. However, looking at the numbers of the entire year, the trend has been somewhat weaker. In 2009 we counted 3,267 different families and 3,313 in 2010.

The topmost places in the rankings were taken by familiar old names, if in a different order. New to the Top 10 are types of fraudulent software and rootkits from the TDSS family, which have become standard in the malware scene.

Families from the online games sector (OnlineGames, Magania etc) were not among the Top 10 most prolific malware families for the first time in the first half of the year.

	# 2010 H2	Virus family	# 2010 H1	Virus family	# 2009 H2	Virus family
1	70,570	Genome	116,469	Genome	67,249	Genome
2	34,412	Buzus	32,830	Hupigon	38,854	PcClient
3	31,834	Hupigon	30,055	Buzus	37,026	Hupigon
4	27,052	FraudPack	25,071	Refroso	35,115	Scar
5	26,013	TDSS	24,961	Scar	24,164	Buzus
6	24,276	FakeInstaller	21,675	Lipler	20,581	Lipler
7	22,411	Refroso	19,385	OnlineGames	19,848	Magania
8	17,535	FraudLoad	17,542	Palevo	18,645	Refroso
9	17,272	BHO	16,543	Startpage	16,271	Sasfis
10	16,645	FakeAV	16,517	Magania	16,225	Basun

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

Genome

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

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 attacked more easily.

Hupigon

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

FraudPack

Trojan horses in the FraudPack family disguise themselves as a wide range of legitimate-looking security tools. However, these tools are anything but secure - they are scareware: The tools serve no security purpose whatsoever and endanger the PC more than help it. Malware in the FraudPack family secretly place additional malicious code on the victim's hard disk - which is why malware is also included among the droppers.

TDSS

Due to its wide range of very technically sophisticated options for disguising malicious files, the TDSS rootkit has become a standard in the malware scene. It is used to conceal files and registry entries for backdoors, spyware and adware.

FakeInstaller

A FakeInstaller involves a fraudulent program that pretends to install popular, legal software. After the usual statements concerning the installation paths, the relevant progress bars appear, ending with a request to send an SMS with specific content to an expensive premium number. The majority of FakeInstallers are operated in Russia.

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.

FraudLoad

The Fraudload family comprises numerous variants of so-called scareware programs, which are presented to the user as security software or system tools. The victim is recommended to have his system scanned for infections. To clear apparent infections, the victim is urged to purchase the "full

version" and thus to divulge his credit card information on a special website. Generally, infection takes place using unpatched security holes in operating systems or via vulnerable application software belonging to the victim. However, there are also attack methods in which the victim is lured to web pages on which it is alleged that videos with erotic content or containing the latest news or gossip can be seen. So that the victim can view the videos, the victim must install a special video codec, which also contains the malware.

BHO

Variants of the BHO family involve plugins for Internet Explorer, which spy on the user. Hence there is generally an attempt to set up secret connections to various servers. The plugin itself is a DLL file, but droppers to install and activate the plugin are also included in the family.

FakeAV

This Trojan horse looks like an antivirus program or another security-related program. It simulates the discovery of multiple security risks or malicious infections on the user's system. This is supposed to trick the user into paying for software to remove the fake alerts.

Platforms: Windows and Web

In recent years the proportion of malware for Windows computers has steadily increased. This also applies to the 2nd half of 2010. However, the proportion of malware that only works on 32-bit versions of Windows has reduced. Yet this is more than compensated for by the sharp increase in malware for modern .NET applications. Both of these groups combined make up 99.5% of all computer malware newly discovered in the second half of 2010.

	Platform	# 2010 H2	Share	# 2010 H1	Share	Diff. 2010H2 2010H1	# 2009 H2	Share	Diff. 2010H2 2009H2
1	Win32	1,056,304	98.1%	1,001,902	98.5%	+5%	915,197	99.0%	+15%
2	.NET	15,475	1.4%	9,383	0.9%	+65%	2,732	0.3%	+466%
3	WebScripts	2,237	0.2%	3,942	0.4%	-43%	4,371	0.5%	-49%
4	Scripts ²	1,111	0.1%	922	0.1%	+20%	1,124	0.1%	-1%
5	Java	517	< 0.1%	225	< 0.1%	+130%	31	< 0.1%	+1.568%
6	*ix ³	382	< 0.1%	226	< 0.1%	+69%	37	< 0.1%	+932%
7	NSIS ⁴	130	< 0.1%	260	< 0.1%	-50%	229	< 0.1%	-43%
8	Mobile	55	< 0.1%	212	< 0.1%	-74%	120	< 0.1%	-54%

Table 3: Top 8 platforms in the last three half-years

The remaining 0.5% is led by web-based malware. Its proportion has significantly reduced however. Reasons for this include the fact that in recent months security holes in Java on websites have been heavily used for running malicious code. This also explains why the proportion of Java malware has increased the most⁵. The proportion of malicious code for Unix-based computers has also significantly increased, whereas the number of families in malware for smart phones has reduced the most.

²"Scripts" are batch or shell scripts or programs that have been written in the VBS, Perl, Python or Ruby scripting languages.

³*ix stands for all Unix derivatives, e.g. Linux, FreeBSD, Solaris etc.

⁴NSIS is the installation platform that is used for installing the Winamp media player etc.

⁵ See also section entitled "Attacks: Java supersedes PDFs"

Trends for 2011

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

Top subjects for the second half of 2010

WikiLeaks brings 'Hacktivists' into the arena

Repeated publication of US government documents - some of them secret - has caused a huge furore and opened a fierce debate on handling data and information. On July 25th the non-commercial website WikiLeaks published the so-called 'Afghan War Diary'. However, revelations on November 28th 2010 exceeded the explosive force of the July documents. In total 251,287 US diplomatic reports ('cables') from 1966 to 2010 were placed on the net, an event now known as 'Cabelgate'. Shortly before they were published, WikiLeaks servers were subjected to DDoS attacks, according to their own reports. One alleged informant is Bradley Manning, Private First Class in the US armed forces, who is facing a 52-year jail sentence if he is found guilty of all charges. According to media reports, the Pentagon has not only forbidden its staff to look at the WikiLeaks documents, but has also blocked access to the US Air Force network for some 25 media sites that have discussed the documents and reported on them.

Because of the public pressure that has arisen, some Internet companies (such as Amazon) have deleted WikiLeaks documents from their web servers or (e.g. PayPal and MasterCard) blocked donor accounts and payment traffic to WikiLeaks. In doing so the companies have incurred the wrath of numerous WikiLeaks supporters. The sympathisers launched 'Operation Payback' and carried out DDoS attacks on Swiss PostFinance, Mastercard, Visa, PayPal, EveryDNS and Amazon. The sites involved were rendered inaccessible for some time as a result. However, according to our research

the attacks were not the result of organised crime. Rather, the attacks led back to WikiLeaks sympathisers, using freely available tools for load testing servers to overload the sites with enquiries. This form of protest has been little used by private individuals to date. These were mostly young men who joined in with the DDoS attacks for idealistic reasons and were mostly unaware that they would have to face legal consequences. In the Netherlands, two men aged 16 and 19 have been arrested in connection with this.

WikiLeaks is not the only platform to be the target of criticism. The spokesman and editor-in-chief of WikiLeaks, the Australian Julian Assange, was meanwhile detained in London on December 7th. He has now been released under caution. However not without being placed under house arrest awaiting extradition proceedings. In Sweden he is due to face charges of alleged sexual misconduct. Assange denies these allegations and describes them as a politically motivated, pre-arranged game. In the USA legal proceedings against Assange are being looked into, but it is not yet known what the reason for the accusation might be. In the media, words such as 'conspiracy' and 'espionage under a law from 1917' are being used. However, it is doubtful whether such laws can be used in the face of the right to freedom of speech which is repeatedly cited.

Industrial facilities at risk: the Stuxnet incident

The Stuxnet computer worm was first reported in July 2010. Its properties were reported incrementally and only following analysis that was at times very exhaustive. The so-called 'LNK security hole' (CVE-2010-2568) was just the tip of this particular iceberg. Details concerning the malware have gradually come to light, only because this hole caused uncontrolled distribution of malicious code from the Stuxnet environment. In total four previously unknown security holes were used to distribute the malware and run malicious code on the target systems using the necessary rights. This did not just involve Windows systems.

Rootkits were installed and stolen certificates used to conceal the malicious files. The target of the attacks is a specific management software package for industrial process management facilities from Siemens. This software uses its own programming language (Step 7) to generate programs with which industrial facilities can be controlled. The malicious function itself is channelled into the control program and generated when the control code for the machinery is compiled. For a long time it was unclear what the actual background to the attacks was. Finally it emerged that the centrifuge for an atomic reprocessing plant in Iran was briefly halted. The short stoppage caused the isotopes to be separated being mixed, thus reducing the quality of the material being prepared. The development of all the code for the Stuxnet malware program required the collaboration of numerous specialists with substantial financial support, taking a total of several man-years. Who is behind the development is unclear and is the subject of much speculation.

The Stuxnet incident showed that there is a circle of people who develop malicious code with substantial financial support to manipulate targeted industrial facilities - even in the area of so-called Critical Infrastructure. The incidents involving Stuxnet illustrate that security problems are not just limited to desktop and server PCs. In principle any control device with an IP address can be exploited.

Security has long been neglected in many industrial facilities. However, the revelations concerning Stuxnet make it clear that thought and attention must be given to this, and not just in the area of infrastructure designated as critical.

Attacks: Java supersedes PDFs

Both the increased proliferation in the area of Java-based malware and the assessment of G Data's monthly Malware Statistics showed a significant change in the threat situation at the end of the year. Online criminals have been relying on security holes in Java to distribute malware more heavily than in previous months. In October the top position in the Malware Rankings changed for the first time since February: Java.Trojan.Exploit.Bytverify.N superseded JS:Pdfka-OE [Expl] for first place in October and was displaced again in December by Java.Trojan.Downloader.OpenConnection.AI, another Java-based threat.

JavaScript-based downloaders like JS:Downloader are also extremely active currently and are constantly being redeveloped by malware authors. Versions of this malware can currently be found in the Top 10 every month.

Security holes in Java offer the perpetrators great technical potential, and the manufacturing and distribution of malicious code is significantly easier compared to other forms of infection - the component elements of the attack can be easily built into so-called exploit kits. Java is found on home and work PCs in huge quantities: in the second half of the year an average of 79% of all PCs had a Java plugin installed⁶.

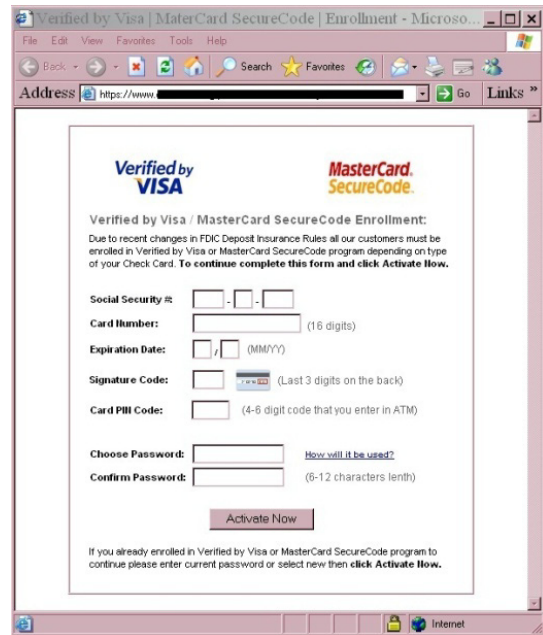
Furthermore, warnings in recent months among users about PDF holes has also led to increased awareness and, thanks to the large number of security updates, the manufacturers of PDF readers have significantly impeded the development of executable malware programs. In particular, innovations in version 10 of Adobe Reader have made it much harder to execute malicious code.

⁶Source: <http://www.statowl.com/java.php>

Events during the second half of 2010

July 2010

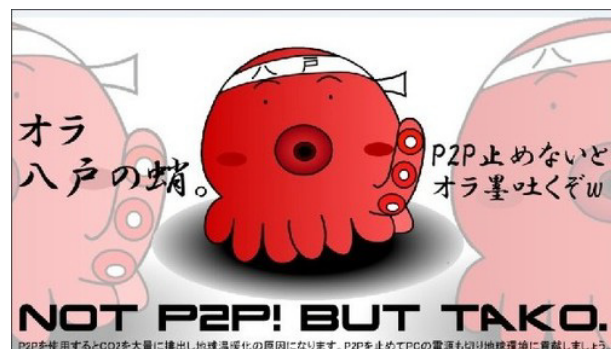
- 13.07. **Microsoft** withdraws **support** for **Windows XP 32-bit Service Pack 2**. Customers should upgrade to Windows Vista or Windows 7 or at least install Service Pack 3 for Windows XP (supported until April 2014). Customers who continue to use Windows XP are more and more in the firing line of cyber-criminals.
- 15.07. The **Zeus banking Trojan** is now also targeting "Verified by Visa" and "SecureCode Protection" credit card security technology. Online banking customers are requested to enter their social security number and credit card information in a fake window injected into the browser - even though this is not actually required in a proper banking process. 15 leading US finance institutes have been targeted by this attack.
- 28.07. The FBI announces that the alleged author of the **Mariposa botnet** has also now been identified and arrested. The 23-year old Slovenian citizen, who goes under the name of 'Iserdo', was caught by Slovenian police. Authorities in Spain, the USA and Slovenia had been scouring the 'butterfly botnet' in persistent investigations lasting two years.



Screenshot 1: The fake Zeus input window for banking information (Source: trusteeer.com)

August 2010

- 05.08. The **Tokyo Metropolitan Police** arrested a 27-year-old man, Masato Nakatsuji, who had been distributing a **computer virus** that deletes all the data on a PC and replaces it with manga-style octopus and squid cartoon images. Before being deleted all the files were sent to a webserver. To date police have identified data from **20,000 users**. Nakatsuji, who had already been convicted of copyright infringement in 2008, did not believe he was in trouble, as this time he had designed the sea-creature images for the **Ikatako virus** himself rather than stealing them.
- 16.08. The Scapegaming company has been ordered to pay over **US\$ 88 million in damages** to the **Blizzard** gaming concern. Scapegaming had set up unlicensed private WOW game servers and allowed these to be paid for by users (around US\$ 3 million in three years). The court delivered a judgment of copyright infringement due to



Screenshot 2: An Ikatako manga (Source: <http://birthofblues.livedoor.biz>)

illegitimate earnings.

- 19.08. Global company **Intel announces** that it is taking over Californian security software manufacturer **McAfee Inc** for a total of 7.68 billion US dollars. McAfee will become a 100% subsidiary of Intel.
- 23.08. **Microsoft** warns of security holes associated with program libraries. Programs could load primed DLL files if they are in the same directory as the file being launched and thus run malware - such attacks are called **DLL spoofing**. The only way currently of at least mitigating the risk is by deactivating the WebDAV service and SMB file sharing protocol. Secunia's list of 160 at-risk programs shows that only 22 have removed the security hole (as of 6/12/2010).
- 28.08. German discount chain **Schlecker** fell victim to a **data leak**. Around 150,000 customer data sets and 7.1 million email addresses for newsletter subscribers were read.

September 2010

- 06.09. The Federal Criminal Police Office and industry association Bitkom estimate the total damage caused by **Internet crime in Germany** in 2010 as **17 million Euro**. Surveys show that around 43% of Germans have been/are affected by a malware infection on their PC. 5% of Internet users to date have suffered **financial loss** caused by malware programs/data theft.
- 08.09. Belgian police confirm that a Europe-wide campaign by **Europol** against **Internet piracy** has been taking place. Investigations, 50 confiscations and arrests were made in 14 European countries. So-called release groups may be responsible for **80% of all new films illegally placed online** in Dutch. They are also accused of distributing copyright-protected music, software and PC games.
- 14.09. Operators of German-language **social network** Lokalisten.de quickly closed a security hole that allowed attackers to run **Cross Site Scripting** on the platform using personal messages. The text filter was unable to filter out the nested JavaScript code.
- 14.09. A **security hole** in an OpenX adserver video plugin enabled criminals to deliver malicious code to websites in **advertising banners** being delivered. Infected banners appeared on sites such as The Pirate Bay, esarcasm and AfterDawn.
- 15.09. The **Federal Agency for Security in Information Technology in Germany** (Bundesamt für Sicherheit in der Informationstechnik - BSI) and eco, the German digital economy association, are today launching their **anti-botnet consultation centre**. It provides software to download, information and advice in the fight against botnets.

20.09. ZoneAlarm's marketing company Check Point is criticised for implementing a form of consumer promotion that was rather unfortunate for the **security industry**: customers of the free ZoneAlarm firewall were encouraged by a pop-up to buy a chargeable complete security package. However, the structure of the **promotion** was very reminiscent of **scareware**.



Screenshot 3: Promotional pop-up in the free ZoneAlarm firewall (source: <http://www.theregister.co.uk>)

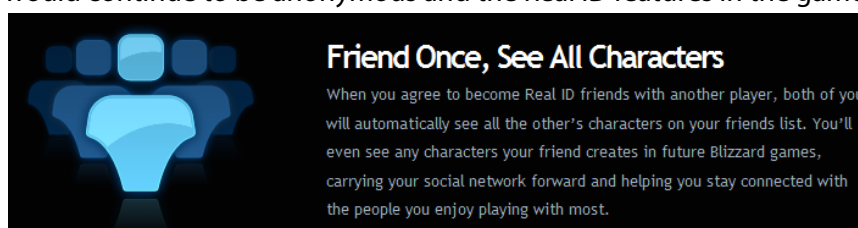
22.09. 49-year-old American Bruce Raisley has been convicted by a court. He had programmed his own malware to recruit around **100,000 zombie PCs** for a botnet. He was using this botnet to run DDoS attacks on web servers that were publishing copies of 2 magazine articles about him. The damage suffered by websites as a result of Raisley's **personal vendetta** was some US\$ 100,000.

23.09. According to NDR, a German **EC card payment** processing company (Easycash GmbH) is not using the data generated during the checkout process in line with the **Federal Data Protection Act**. Instead it is using the data to make extrapolations enabling assertions to be made about a cardholder's ability to pay and his or her creditworthiness.

24.09. **UNICEF**, the United Nations International Children's Emergency Fund, unintentionally placed a list on the Internet containing data on 147 companies involved in the "Spenden statt Schenken" campaign ("donate instead of sending presents") in 2009. The data became accessible via the Google search engine. The cause of the data mishap was a server migration during which security settings were incorrectly carried out.

27.09. The **PayPal** online payment service comes under pressure after it is revealed that it was possible to carry out transactions of up to **1,500 Euro** without any real difficulty using third-party credit card data. **Verification of customer data** can take time and during this time "there is no limit on payment, receiving and sending of funds", according to a spokeswoman.

30.09. **Blizzard** announced in July that in future all contributions in its own forums will show gamers' real names (**Real ID**). This and other features of this type are intended to make games **more like social networks**. The gaming community reacted negatively. For example, one user published a range of personal data on Activision/Blizzard employees in his blog, found on the Internet using Real ID (including marital status, address, names of relatives etc). **Blizzard has now changed the plans it announced**, to the effect that forum contributions would continue to be anonymous and the Real ID features in the game would be optional.



Screenshot 4: Description of one of the Real ID functions (source: us.battle.net)

October 2010

- 01.10. The **FBI** successfully concluded **Operation Trident BreACH**, which was initiated over 18 months ago against cyber-criminals and primarily the **Zeus botnet**. In recent days 16 search warrants were enforced and 39 targeted arrests were made in the USA, Netherlands, Ukraine and United Kingdom. The total money stolen amounts to 220 million US dollars.
- 09.10. According to media reports, **customs officers** in Germany are being permitted to **listen in to VoIP telephone calls** with judicial approval and act on them in line with the decree of the Federal Constitutional Court on so-called online investigation. Investigators secretly run a program to access the suspect's computer and tap into the verbal data **before it is encrypted**.
- 17.10. The US website of AV manufacturer **Kaspersky** today distributed **scareware** to Internet users for almost 4 hours. Hackers are using a vulnerability in a third party provider's application to forward customers intending to download Kaspersky products to an infected website with FakeAV.
- 22.10. The **US government's Cyber Command**, launched in May, is now on duty. The precise remit of the special unit, based in Ft. Maede, Maryland, is still unclear, however. President Obama said in May: "It's now clear this **cyber-threat** is one of the most serious economic and national security challenges we face as a nation." However, he asserted that the new special unit would not be monitoring private networks or email accounts - that was not its meaning and purpose.
- 27.10. **Mozilla** reported a critical security hole in its Firefox 3.5 and 3.6 browsers that was first being exploited by hackers to load a Trojan horse onto the **Nobel Peace Prize website** that would run on the victim's computer as a **drive-by download**. The vulnerability was closed within 48 hours via a browser update to 3.6.12 and, according to reports, only applied to users of Windows 2000 and Windows XP.
- 29.10. **'Katusha', the investigation commission** has succeeded in **infiltrating an international group** that has been manipulating online banking transactions on a large scale. The people behind this were investigated in collaboration with Estonian and British authorities and are said to have manipulated over 260 transactions and **acquired at least 1.65 million Euro**. The victims' PCs were infected with manipulated PDF files and malware from drive-by downloads.



Screenshot 5: The official logo of the US Cyber Command

November 2010

- 04.11. The alleged operator of the **Mega D botnet** has been arrested. Oleg Nikolaenko, a 23-year-old Russian, was caught by the FBI in Las Vegas. For some time it has been unclear whether he was hiding alone behind the botnet, which is claimed to be responsible for **19% of spam sent worldwide** - according to SPAMfighter, in 2008 a full 32% led to the Mega D account. Nikolaenko, from Moscow, will be charged with infringing the Can-Spam act.
- 05.11. The so-called **'Origami Trojan'** is distributed primarily in Russia and the Ukraine. The 'very powerful Trojan', which primarily steals **personal data**, has been focusing on **bank data**. It is unusual for malware that allegedly comes from Russia or the Ukraine to attack computers there as well - it contradicts an unwritten law.

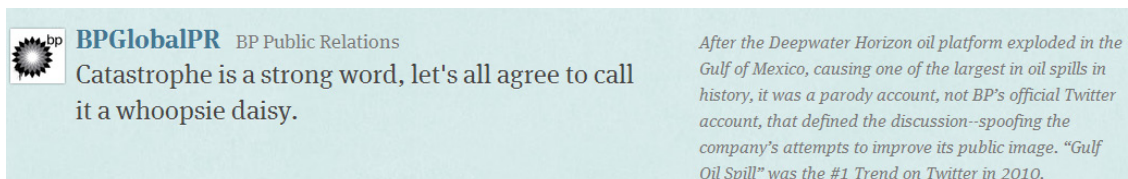
- 8.11. In Florida (USA), the police caught up with a **burglar** because he had forgotten to log out of his **MySpace profile** - he had used a computer in a bedroom in the house he had broken into. The 18-year-old was arrested in the vicinity of the house.
- 09.11. Less than 24 hours after the launch of **software for the new German electronic identity card**, a security hole was discovered. Unlike in tests by the Chaos Computer Clubs (CCC), the user's computer did not now have to be contaminated with malicious code. According to statements from blogger Jan Schejbal, attackers can use their own SSL certificates to trick the application's update function and plant their own malicious software on users.
- 12.11. 22-year-old **David Kernell**, who hacked into **American vice-presidential candidate Sarah Palin's** private email account in 2008 (among other things) was today sentenced to jail for one year and one day. A judge from the US Justice Department said Kernell's act was "a political act, with political motives, intended to derail a political campaign." Kernell had gathered personal information about Palin on the Internet and used it to answer the **security question** for her email account. He then published images and emails from Palin and ensured they could be seen across the world.
- 18.11. Google launches its new **Google StreetView** service. The controversial project, which was the cause of much excitement at the beginning of the year, today activated **images of 20 German cities** that the user can travel through virtually. According to media reports, before the launch **250,000 people registered their opposition** to the publication of images of their houses. Google promised to make number plates and faces generally unrecognisable.
- 18.11. **G Data SecurityLabs** experts discover a **potential successor to the Zeus Trojan**. The malware's author is advertising his Trojan horse in a forum and is promising a speedy release. As the description of the malware promises **a great number of variants**, it could be used for practically any target of attack. A starter pack is said to be available for US\$ 850.
- 23.11. 33-year-old Scot Matthew Anderson was running a **botnet** from his mother's living room and using it to send millions of spam emails, steal personal data from victims' computers and even spy on victims using their webcams. The father of five did not even have broadband Internet access in his own house. He was sentenced to a **£5,000 fine and 18 months in jail**.
- 24.11. The **French government** wants to introduce a tax on the "purchase of online advertising services" from January 1st 2011. This tax will have to be paid by the online businesses that accept the contracts - but only those based in France. The government anticipates revenues of 10 to 20 million Euro per year from the so-called '**Google tax**'.
- 28.11. **WikiLeaks** publishes almost a quarter of a million **US diplomatic cables** on the Internet - some classified as secret. In association with this, two young men of 16 and 19 were detained in the Netherlands in December. WikiLeaks spokesman **Julian Assange** is meanwhile detained and later placed under arrest. There is detailed information on this in the section entitled 'Top subjects for the second half of 2010'.



Screenshot 6: The Ares Command & Control Interface

December 2010

- 01.12. Two men from North Rhine Westphalia in Germany are accused of a specific type of **music piracy**. A 17-year-old and a 23-year-old gained access to email accounts belonging to people **prominent in the field of music** and stole music not yet published. They are said to have used Trojan horses to distribute **infected MP3 files** in order to gain access to computers. The police intervened when the men showed off their booty in a Kelly Clarkson online fan club.
- 3.12. The Grand Chamber of the **Swiss parliament** is addressing the **security of important communications and data networks**. It is calling for laws for active and passive security for these. The Defence Minister also sees the **need for action in relation to the areas of cyberwar and cyberdefence** - coordination arrangements need to be made. The Green politicians consider a blanket law to be difficult as citizens should not be allowed to be restricted.
- 10.12. A 44-year-old man from Dülmen (Germany) has been sentenced to **a one year and 10 months suspended sentence** for using a Trojan horse to access **almost 100 private computers** and **watch the owners using their own webcams**. The youngest victim was a 13-year-old girl, who noticed after a while that the indicator light on her webcam never went off and reported it.
- 14.12. In **Colorado (USA)** the Sheriff's Department fell victim to an extensive **data leak**. **200,000 sets of data** on suspects, victims and informers could be accessed online without protection. After being copied to a computer believed to be secure in April by a member of the department, the data became unintentionally public and so presented a potential **risk to the people listed**. The data leak came to light in November, when one person on the list found his own name on the Internet.
- 18.12. The micro-blogging service **Twitter** publishes its **annual statistics for 2010**: 1st place in the Top Trends goes to the oil catastrophe in the Gulf of Mexico, followed by the FIFA football World Cup and the cinema release Inception. Even Paul the Octopus featured in the **Top Ten** - if only in 10th place. 4th place in the '**most powerful tweets**' went to a commentary on the Deepwater Horizon catastrophe, twittered by a parody account:



bp BPGlobalPR BP Public Relations
Catastrophe is a strong word, let's all agree to call it a whoopsie daisy.

After the Deepwater Horizon oil platform exploded in the Gulf of Mexico, causing one of the largest in oil spills in history, it was a parody account, not BP's official Twitter account, that defined the discussion--spoofing the company's attempts to improve its public image. "Gulf Oil Spill" was the #1 Trend on Twitter in 2010.

Screenshot 7: Somebody created a parody account to post tweets like this referring to the oil catastrophe (source: <http://yearinreview.twitter.com/powerful-tweets/>)

- 25.12. US **magazine TIME** names Facebook founder **Mark Zuckerberg** as **Person of the Year for 2010**. He changed society and united over 550 million people worldwide - some 70% of Facebook users live outside the USA. On the other hand, British financial newspaper the **Financial Times** considered **Steve Jobs** the most outstanding personality of 2010.
- 28.12. The chief of police in **Zuidwest-Drenthe** (Netherlands) was suspended for an unsuitable **Twitter contribution**. She had prematurely tweeted speculations on the cause of death of two females and thereby potentially infringed the victims' personal rights.