

German  
Data  
Security



# G Data Malware Report

Half-year report January - June 2009

Ralf Benz Müller & Werner Klier  
G Data Security Labs



Go safe. Go safer. G Data.



## At a glance

### Facts and figures

- In the first half of 2009, G Data identified 663,952 new malware programs, which is more than twice as many as in the comparable period of last year. Relative to the second half of 2008, only a slight increase of 15% could be achieved. By contrast, the number of active malware families fell by 7%.
- The most common malware categories are Trojan horses, backdoors and downloaders. While Trojan horses and downloaders were able to build upon their positions, the share of backdoors fell back. Rootkits further strengthened their positions. Their number increased relative to the same period last year by a factor of 8.
- Malware with its own distribution routine makes up only 4.0% of all computer malware.
- Amongst the most frequent malware types are Trojan horses, backdoors and online-game account stealers. Occurrences of the worm family "Autorun" have also increased noticeably. Numbers are up by a factor of nearly five times in comparison with the first half of 2008 and their share has increased to almost 1.6%.
- 99.3% of all malware discovered in the second half of the year runs under Windows. Concentration on the operating system market leader continues.
- Malware for mobile platforms has managed to climb into the top 5 platforms for the first time. However with 106 malware programs, its share is still at a very low level.
- Users of MacOS X are also being attacked by Malware. There are 15 new malware programs for MacOSX. In April, a botnet based on Apple computers was discovered for the first time.

### Results and trends

- Social networking services are increasingly used for spreading spam and malware.
- Conficker is becoming a household name. It infected several million PCs and on the 1st April made the headlines again with a new update routine. Since then it has been quiet.

### Outlook

- Ever more malware is shifting into the Internet. Infection methods are becoming ever more sophisticated.
- The malware flood will continue to increase in the coming months, but with slower growth rates and supported by fewer malware families.
- Users of MacOSX and smartphones are increasingly being targeted by malware authors.

# Contents

<b>At a glance</b> .....	<b>2</b>
Facts and figures .....	2
Results and trends .....	2
Outlook .....	2
<b>Contents</b> .....	<b>3</b>
Events and trends of the second half of 2008.....	3
Calendar .....	3
Malware: Facts and figures .....	3
Outlook for 2009 .....	3
<b>Malware: Facts and figures</b> .....	<b>4</b>
The malware flood is still increasing - but no longer so strongly.....	4
Malware Categories .....	4
Family ties.....	6
Platforms.....	8
<b>Outlook for 2009</b> .....	<b>9</b>
Outlook .....	9
<b>Events and trends of the first half of 2009</b> .....	<b>10</b>
January 2009 .....	10
February 2009 .....	11
March 2009 .....	13
April 2009 .....	14
May 2009 .....	15
June 2009 .....	15

# Malware: Facts and figures

## The malware flood is still increasing - but no longer so strongly

In the past few years, the number of new malware programs has increased continuously. Ever increasing growth rates mean that new records are constantly being set. Also in the first half year of 2009, the number of computer malware programs has grown again. In comparison with the same period last year, the number, at 663,952, has more than doubled. However, as already reported in the last G Data Malware report, the growth rate has reduced. In comparison to the second half of 2008, the number of malware programs has only increased by 15%.

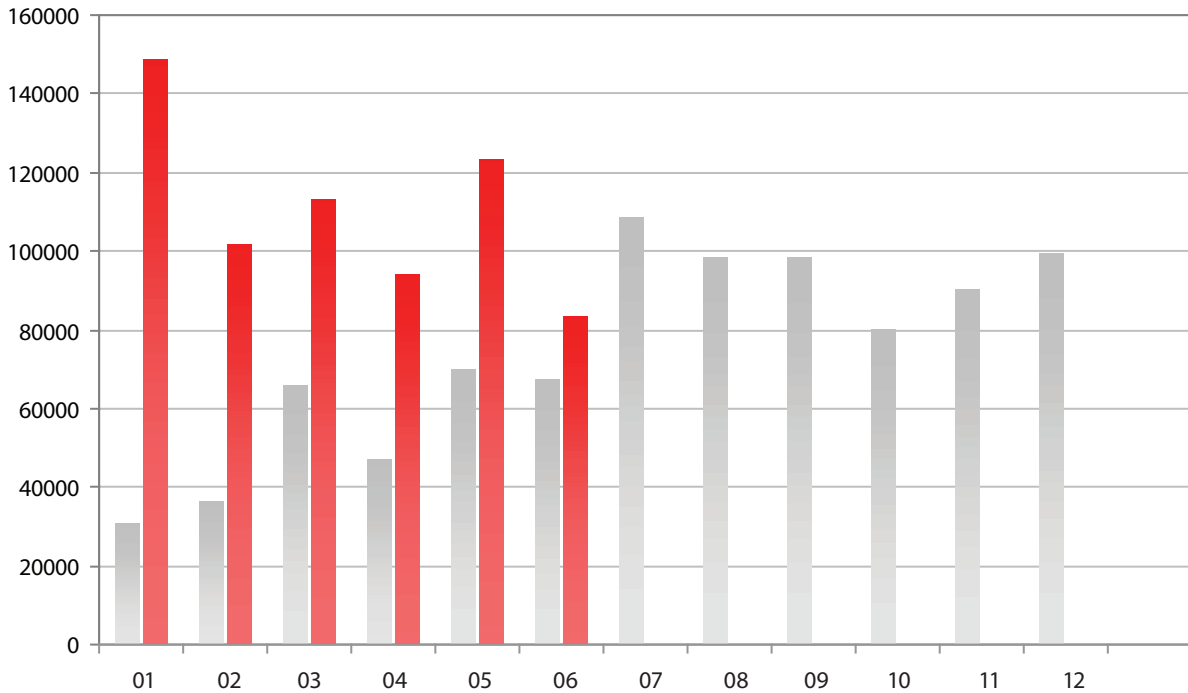


Diagram 1: Number of new malware threats per month for 2008 (grey) and 2009 (red).

## Malware Categories

A glance at the changes in the individual malware categories provides explanations for this fall-back. While backdoors, adware and spyware remain below average, the quantity of rootkits and Trojan horses have considerably exceeded the average increase. The number of downloaders and droppers is also above average.

Backdoors are needed to integrate zombie computers into a botnet so that they can be remotely controlled. A fallback in this area is evidence that the development of botnets has lost some of its importance. The significant increase in rootkits indicates that ever more malware (also backdoors) are hidden from virus protection and prying eyes. Apparently the available capacity suffices to meet the demand for botnet activities such as sending spam and executing denial of service attacks. The adware market also appears to be stagnating at high levels. Possibly awareness campaigns are having some effect here. However, the economic crisis that has persisted in the medium term is contributing to the fact that even participants in the eCrime economy must cut their cloth according to their needs.

The number of spyware programs has reduced slightly. More closer investigation reveals that the number of keyloggers has doubled, while banking Trojans and data theft for passwords or

online games have each reduced by some 30%. The increased security procedures of banks and online games operators are no longer easily circumvented using simple means. Where data theft is concerned, the trend is towards ever more universal and high-performance malware.

Category	#2009 H1	Share	#2008 H2	Share	Diff 2008H1 2008H2	#2008 H1	Share	Diff 2008H1 2009H1
Trojan horses	221.610	33,6%	155.167	26,9%	143%	52.087	16,4%	425%
Backdoors	104.224	15,7%	125.086	21,7%	83%	75.027	23,6%	139%
Downloaders/droppers	147.942	22,1%	115.358	20,0%	128%	64.482	20,3%	229%
Spyware	97.011	14,6%	96.081	16,7%	101%	58.872	18,5%	165%
Adware	34.813	5,3%	40.680	7,1%	86%	32.068	10,1%	109%
Worms	26.542	4,0%	17.504	3,0%	152%	10.227	3,2%	260%
Tools	11.413	1,6%	7.727	1,3%	148%	12.203	3,8%	94%
Rootkits	12.229	1,9%	6.959	1,2%	176%	1.425	0,4%	858%
Exploits	2.279	0,3%	1.841	0,3%	124%	1.613	0,5%	141%
Diallers	1.153	0,2%	1013	0,2%	114%	4.760	1,5%	24%
Viruses	143	0,0%	167	0,0%	86%	327	0,1%	44%
Miscellaneous	4.593	0,7%	8.419	1,5%	55%	5.170	1,6%	89%
Total	663.952	100,0%	576.002	100,0%	115%	318248	100,0%	209%

Table 1: Number and proportion of new malware types in the first halves of 2008 and 2009 together with the overall change

Table 1 shows that the number of diallers has fallen to scarcely a quarter of the previous year's volume. Evidently the dialler business model is becoming obsolete. Also the number of classical viruses (i.e. file infectors) has decreased considerably in comparison with the same period last year. This distribution path is now the exception rather than the rule. The worms - including the large group of Autorun infectors - were able to increase their share to 4.0%. This number has increased by a factor of 2.6 in comparison with the first half of 2008 and by factor of 1.5 in comparison with the second half of 2008.

## Family ties

Based on the functions and properties of the program code used, malware programs are sub-divided into families. The number of virus families has been reducing for years. In the first half of 2008 there were still 2395, while in the second half, it was down to 2094. In the first half of 2009, a total of 1948 different examples of virus families were counted. I.e.: the once again increased malware figures are based on a reduced number of families. This indicates a concentration of the market.

	#2009 H1	Virus family	#2008 H2	Virus family	#2008 H1	Virus family
1	45.407	Monder	45.407	Hupigon	32.383	Hupigon
2	35.361	Hupigon	35.361	OnlineGames	19.415	OnLineGames
3	20.708	Genome	20.708	Monder	13.922	Virtumonde
4	18.718	Buzus	18.718	MonderB	11.933	Magania
5	15.937	OnlineGames	15.937	Cinmus	7.370	FenomenGame
6	13.133	Fraudload	13.133	Buzus	7.151	Buzus
7	13.104	Bifrose	13.104	Magania	6.779	Zlob
8	12.805	Poison	12.805	PcClient	6.247	Cinmus
9	11.530	Magania	11.530	Zlob	6.194	Banload
10	10.412	Inject	10.412	Virtumonde	5.433	Bifrose

Table 2: Top 10 most active virus families in the first half of 2009 and in both halves of 2008

While for some families, there are only a handful of variants, others are particularly productive. Some of them have been present in the top 10 for years. These include backdoors belonging to the Hupigon and Bifrose families, which have lost their top position, the online games data stealers from the OnlineGames and Magania families as well as the Trojan horses belonging to the Buzus family. The new front-runners are the Monder adware/scareware Trojans, which are following in the footsteps of Virtumonde. Together with the new entry, Fraudload, they indicate how popular scareware with its imitation virus protection solutions has become with cyber criminals. Also new to the top 10 are the families Genome, Poison and Inject.

**1st place: Monder**

The countless Monder variants are Trojan horses, which manipulate system security settings on the infected system and can thus make the system more susceptible to further attacks. Additionally an infection can take place using adware, which displays unwanted advertisements on the infected system, especially for counterfeit security software. 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 to pay by credit card!! Some variants download further malware and transfer information to the attacker about the victim's surfing behaviour, without informing the user of such action.

**2nd place: Hupigon**

Amongst other things, the Hupigon backdoor allows the attacker to remotely control the computer, record keyboard entries, access the file system and switch on the webcam.

**3rd place: Genome**

The Trojans of the Genome family combine functionalities such as those of downloaders, keyloggers and file encryption.

**4th place: Buzus**

Trojan horses from the Buzus family scan the infected systems of their victims for personal data (credit cards, online banking, email and FTP accesses), which are then transferred to the attacker. Not only that, the malware attempts to lower the computer's security settings so that the victim's computer can be more easily attacked.

**5th place: 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. The attacks primarily target games which are popular in Asia.

**6th place: 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 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.

**7th place: Bifrose**

The Bifrose backdoor provides attackers with access to infected computers and connects to an IRC server, from which the malware program receives the attacker's commands.

**8th place: Poison**

The poison backdoor provides attackers with unauthorised remote access to the victim's system, which can then be exploited for distributed denial of service attacks (DDoS).

**9th place: Magania**

Trojan horses from the Chinese Magania family have specialised in the theft of gaming account data from the Taiwanese software producer, Gamania. In general, Magania examples 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.

**10th place: Inject**

The inject family contains a large number of Trojan horses, which insert themselves in running processes and can thus take control of the respective process. This allows the attacker to maliciously manipulate the compromised processes at his will.

The most active **worm family** is "Autorun" with 9,689 variants and a share of 1.6%. Representatives of this family use the mechanism which, upon insertion of CDs/DVDs or connection of USB data media, automatically executes files. Accordingly it copies itself onto the data medium and creates a file called autorun.inf. Due to the wide distribution of this malware, it is advisable to deactivate the Windows autorun mechanism. So that this really works, Microsoft has produced its own patch.

The most frequently occurring **Exploits** relate to WMF security holes and weak points in PDFs. The number of harmful PDF files has increased greatly in the last few months. In this respect it is not only security holes which are exploited. The possibility of executing JavaScript code in PDFs is also enjoying increasing popularity amongst malware authors.

## Platforms

In the first half of 2009, malware authors once again concentrated on attacking Windows computers. At 99.3% the fraction of Windows malware increased once again. Malware for other operating systems remains extremely scarce. For Unix-based systems, 66 malware programs appeared (in comparison with 16 in the second half of 2009), while for Apple's OSX, only 15 new malware programs were found. In the second half of 2008 it was 6. Even if an increasing trend in malware for other operating systems is identifiable here, its share in comparison with the flood of windows malware is negligible.

	Platform	#2009 H1	% 2009 H1	#2008 H2	% 2008 H2	#2008 H1	Share
1	Win32	659.009	99,3%	571.568	99,2%	312.656	98,2%
2	WebScripts	3.301	0,5%	2.961	0,5%	3.849	1,4%
3	Scripts	924	0,1%	1.062	0,2%	1.155	0,3%
4	MSIL	365	0,1%	318	0,1%	252	0,1%
5	Mobile	106	0,0%	70	0,0%	41	0,0%

Table 3: Top 5 platforms in 2008 and in the first half of 2009. WebScripts refer to malware that is based on JavaScript, HTML, Flash/Shockwave, PHP or ASP and usually exploit weak points via the browser. "Scripts" are batch or shell scripts or programmes that have been written in the script languages VBS, Perl, Python or Ruby. MSIL is malware stored in the byte code of .NET programmes. Mobile encompasses malware for J2ME, Symbian and Windows CE.

The number of new malware programs for smartphones and portable computers has grown by approximately a half, while malware for portable devices has again made it into the top 5. Overall, 106 new malware programs have surfaced. Approximately 90 of these programs have no propagation routine of their own and are primarily used to send text (SMS) messages to Russian and Chinese telephone customers. Only the Yxe family spreads independently via text (SMS) messages with a link to a website. The file, which is offered for download there, is signed by Symbian. Thus, as previously, the only required user action is reduced to a click.

## Outlook for 2009

Malware will again earn a lot of money in the coming months. The eCrime economy is firmly established and the proven business models based on spam, spyware and adware will ensure that the tills continue to ring for the writers, distributors and exploiters of malware. And once again, the occasional success of the law enforcement agencies isn't going to change anything. Windows users will continue to be targeted by cyber criminals.

The malware flood will continue to rise. However it is conceivable that the increasing numbers will originate from ever fewer malware families. The measured rates of increase are no longer as great as in past years.

In view of the the professional approach of the black economy, it is no wonder that security holes in the the operating system and popular applications are exploited by malware only a few days after their release. In no time at all, easy-to-use tools are also available for inexperienced users which permit the creation of malware. Currently the weakest link in the chain is the browser and its components. This is where most security holes are found and exploited. If you don't keep you computer up-to-date, then you are offering malware attackers a much bigger target.

However experiments on other platforms are set to continue. The number of malware programs on Apple, Unix and portable computers will increase. However mass exploitation is not expected.

As by now, many malware gateways have been closed by security technologies, the attackers are shifting to less well protected areas. The largest chances of success in this respect are currently offered by websites with their numerous applications. Therefore it is to be expected that in the coming months newer and ever more devious attack scenarios will be exploited. In this respect currently underrated media such as Flash or PDF will be more strongly exploited. Also the bag of tricks with which con-artists entice web surfers to visit a web page or execute files will certainly continue to grow. We particularly expect such deceptive approaches where social networks are concerned. Currently, Twitter offers most opportunities in this respect.

## Outlook

Category	Trend
Trojan horses	↗
Backdoors	→
Downloaders/droppers	→
Spyware	→
Adware	→
Viruses/worms	↘
Tools	↗

Category	Trend
Rootkits	↗
Exploits	↗
Win32	↗
WebScripts	↑
Scripts	→
MSIL	→
Mobile	↑

## Events and trends of the first half of 2009

Here we present the most important events associated with malware in chronological order. The most prominent events are those associated with Conficker, which caused a huge commotion in the first few months of the year. Also conspicuous are the many incidents amongst the favourite social networking services such as Twitter, LinkedIn, MySpace and Facebook. In the meantime malware designers are very quickly aware of such trends and use the opportunities they provide. Apart from individual incidents, other trends also demonstrate that social networking services are gaining in attraction. While a year ago phishing was largely limited to banks and eBay, in the last half year Google and the social networking sites Facebook, Sulake and MySpace have become permanent members of the phish tank top 10. For some time social networking sites have served cyber criminals as sources of information in the preparation of targeted attacks and personalised spam. Social networking sites are becoming ever more popular, which is also true for malware programmers.

This is clearly demonstrated by development of the **Koobface** worm. If in the beginning, it was, as its name suggests, concentrated on Facebook and shortly thereafter on MySpace as a distribution platform, then the list has been expanded in the last few months by social networking sites such as hi5.com, friendster.com, myyearbook.com, bebo.com, tagged.com, netlog.com, fubar.com and livejournal.com. The links created there point to websites where the proven defrauding template "Schummel AntiVirus" or "Codec/flash download" can be sampled. But Koobface is also expanding in numbers, as the following table shows. In June the number of variants went up by a factor of nearly ten.

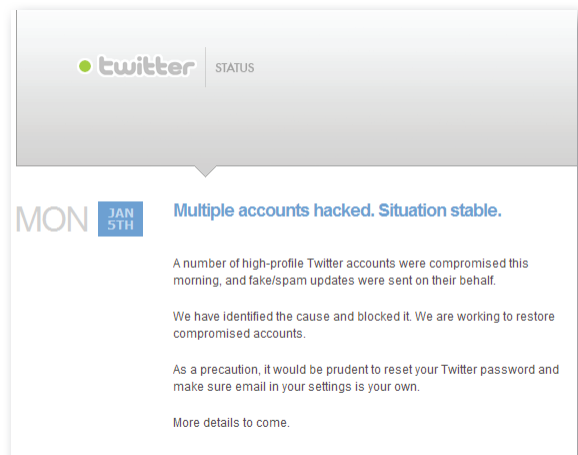
Month	Jan 09	Feb 09	Mar 09	Apr 09	May 09	Jun 09
# Koobface variants	18	14	23	50	56	541

Table 4: Number of Koobface variants in the first half of 2009

In the coming months we expect more malware on social networking sites. With the increasing user numbers, the attraction to malware distributors also climbs.

### January 2009

- 05.01. Users of the micro-blog site Twitter are attracted to a counterfeit login-page for the service so that access data for future spam campaigns can be stolen.
- 06.01. **Twitter** warns: "Multiple accounts hacked. Situation stable". Amongst the accounts affected are those of Britney Spears and Barack Obama. Partially salacious messages are sent under the name of the victim.



- 07.01. False celebrity profiles are created on the social networking site **LinkedIn**. They contain links which point to counterfeit virus scanners or a version of Windows Media Player contaminated with a Trojan horse. Prominent victims: Victoria Beckham, Beyoncé Knowles, Salma Hayek and lots more
- 08.01. 3000 computers of the Austrian federal state of Carinthia are infested with the **Conficker** worm. Reason: the security update published by Microsoft in October 2008, which should close a security hole exploited by Conficker has not been installed up until now.
- 12.01. **Conficker** strikes again in Carinthia, this time in the hospitals of the Carinthia Hospital Association KABEG. Again some 3000 computers are affected.
- 14.01. Estimates of up to 2.5 million **Conficker** infections already. For the first time it is recognised that Conficker uses a special algorithm to generate permanent domain names, with which contact is made at random. Objective: the attackers have registered many of these random domains in advance and can use them to download further malware or provide infected computers with further instructions.
- 21.01. The **Conficker** epidemic continues unabated: large parts of the British armed forces are affected.
- 23.01. A Trojan copy of the Apple layout and presentation software **iWork 09** circulates in the BitTorrent network. Some 20,000 users are believed to have downloaded the distributed copy since the beginning of the month.
- 25.01. The job site **Monster.com** informs the public that it has suffered from a data theft attack. "Unpermitted access" to the company's database means that access data, names, telephone numbers, email addresses and some demographic data have been captured.

## February 2009

- 01.02. Due to a security hole in the beta version of **Windows 7**, a simple script can be used to disable the user account control (UAC), so that operating system attackers can plant further malware code unobserved.
- 02.02. Attackers manipulate the website of the **Hamburger Abendblatts**, so that visitors to the site's pages can be infected with malware.
- 04.02. Using a false login page of the RTL social networking site **wer-kennt-wen.de**, user login data are spied on.
- 08.02. Using a targeted distributed **denial of service** attack, various security websites such as Metasploit, Milw0rm or Packetstorm are rendered temporarily lame.
- 10.02. Only two days after the first attack, the website of the **Metasploit** project is again targeted by a DDoS attack. The attackers vary the attack technique multiple times.
- 11.02. Via a security hole in the content management system **Typo 3**, the existence of which was only identified one day before, various German-speaking websites, which have not yet loaded the appropriate security update, are manipulated. Affected for example are

the web pages of **FC Schalke 04**, on which the departure of Kevin Kuranyi is reported, or the website of Wolfgang Schäuble on which a link to the topic of data retention is placed.



- 12.02. **Microsoft** puts up a **bounty** of 250,000 dollars for the arrest and punishment of the author of the **Conficker** worm. Simultaneously the software manufacturer announces that to limit the spreading infection it will collaborate closely with ICANN and the operators of central DNS servers.
- 14.02. Several hundred computers of the Bundeswehr are infected with **Conficker**.
- 17.02. Due to an incorrect router configuration at a Czech Internet provider, data transfer stability in some parts of the global Internet are significantly impaired.
- 23.02. Malware researchers analyse the variants B and B++ of the Conficker worm and determine that, due to its modular design, it can act in a much more flexible manner than the original variant A.
- 25.02. Using a primed flash banner, attackers distribute manipulated PDF documents via the website of the online magazine eWeek and other online sites of the Ziff-Davis network that install counterfeit antivirus software on the victims' computers.

## March 2009

- 01.03. Malware researchers decode the algorithm that **Conficker** uses to generate the domain names of a control server. It also produces names that have already been used. During March, the legitimate domains jogli.com (music search machine), wnsux.com (Southwest-Airlines), qhflh.com (Chinese women's network) and praat.org (audio-analy-

sis) are disrupted by connection attempts from Conficker computers.

- 04.03. A team of specialists from LKA Baden-Württemberg shuts down the illegal trading platform **codesoft.cc** on which Trojan horses and illegal information about the stealing of data and forging of credit cards is offered for sale.



- 09.03. **Conficker** uses a new algorithm, which now calculates, rather than 250 domains a day, 50,000 domains a day. Moreover processes are ended on infected computers, which contain certain character chains, that are associated with analysis tools that are specially directed against the worm. The malware program thus actively defends itself against measures designed to contain the epidemic.
- 12.03. The British **BBC** takes over control of a **botnet** with some 22,000 computers in the course of research. As cases against the BBC result from the takeover, the latter announces that the research is in the public interest and is thus covered by the guidelines of the British media supervisory authority, OFCOM. The question as to whether money was paid to take over the botnet remains unanswered by the BBC.
- 17.03. By use of the authentic domain [dhl-packstation.info](http://dhl-packstation.info), Internet criminals lure **Packstation** users to a counterfeit login page so that it can spy on their login data.
- 23.03. **DSL-routers** of type Netcomm NB5 can be manipulated via a web interface and SSH access from the Internet without a password due to obsolete firmware and form a botnet called **Psybot**, the size of which is estimated at 80,000 to 100,000 infected routers.
- 30.03. According to expert statements **Conficker** will start to



search through countless domains generated by its algorithm on the 1st April. What exactly will happen upon establishing of contact, nobody can say at this point in time.

- 31.03. The broad media interest in **Conficker** gives feeloaders the idea of carrying out targeted manipulation of web pages with apparent disinfection tools so that they then appear in the hit lists of the Google search machine. In reality the purportedly helpful tools are **Scareware**, i.e. counterfeit antivirus software, which suggests to the victim that their computer is infected and tries to discover their credit card information.

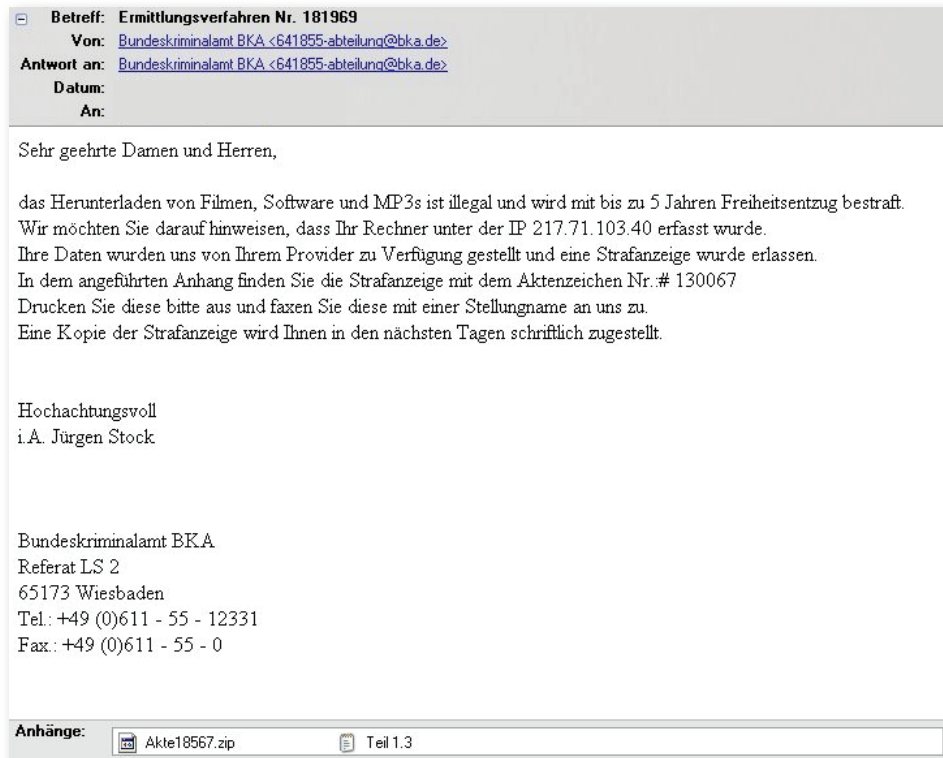
## April 2009

- 01.04. The expected update attempts of **Conficker** go nowhere at first. Apparently infected systems make contact with certain domains as expected in the run-up. However probably at this point in time no update is yet available.
- 09.04. Contrary to the original expectations, **Conficker** does not load updates from the domain names generated by an algorithm. Rather it falls back on an alternative P2P mechanism and uses it to communicate directly with other infected systems. The new variant blocks, in a targeted manner, access to the websites of antivirus producers, so that access to special removal tools is made more difficult.
- 12.04. **Conficker** loads the scareware "SpywareProtect2009" from a Ukrainian server, which then gives out false virus warnings on the victims' computers. For removal of the reported (and de facto non-existent) malware, the afflicted user should pay 49.95 dollars.
- 18.04. Security experts discover the indications of a first **Apple computer botnet**. Apparently there is a link to the Trojan version of Apple's iWork 09 which appeared in the BitTorrent file sharing service at the start of the year. In addition a Trojan version of Adobe Photoshop CS4 is likewise circulating.
- 22.04. The **largest ever detected botnet** in the world is traced. It contains almost two-million infected zombie PCs. The operator is probably one of a gang that comprises only six people, who operate the corresponding Command & Control server in the Ukraine.
- 23.04. In the Russian part of the World Wide Web a **Trojan horse** surfaces that locks users out of their Windows PC and demands a **ransom** for the release of their computer. Affected users must send a text message to a particularly expensive premium number in order to obtain a release code.

## May 2009

- 07.05. A study by the telecommunications group, BT, discovers that second-hand **hard disks** are insufficiently cleaned before they are sold on and may sometimes contain extremely sensitive data. In a test purchase of 300 used hard disks confidential details of a test series of US-American rocket defence system as well as blueprints of the US defence group, Lockheed Martin, were found.
- 08.05. According to a report of the US FAA, in the last few years **hackers have penetrated the air traffic control system** several times. The extent extends from illegal access to nearly 50,000 personal data records for FAA employees up to the possibility of turning off the power supply to important servers.
- 09.05. Falsified installation packages for an apparent release candidate of **Windows 7** contain a **Trojan horse**, which is activated during the execution of the setup.

- 24.05. The **Bundeskriminalamt** (BKA - Federal Criminal Police Office) warns of falsified emails, which are distributed in its name and demand that the recipient pays a fine as a consequence of a criminal charge brought by the BKA as a result of the illegal downloading of films, software and MP3 files.



- 30.05. A report by the magazine InformationWeek lets it be known that Turkish activists have, on multiple occasions, **captured US Army web servers**. Accesses to the affected web pages were redirected to other web pages that contained political slogans.

## June 2009

- 03.06. Some ten thousand legitimate websites fall victim to a **mass hacking** event. Visitors to the manipulated websites are redirected to a Ukrainian server, which distributes exploits for Internet Explorer, Firefox and Quicktime.
- 05.06. The Californian Internet service provider **Pricewert LLC**, which also operates under the aliases **3FN** and **APS Telecom**, is removed from the Net under pressure from the American Federal Trade Commission (FTC). Alongside the housing of command & control servers for control of over 4,500 spyware programs, the company is said to have actively recruited criminals and made the tracking of illegal content more difficult. In contrast to the dramatic shutdown of McColo in November 2008, this action has only a minimal effect on the distribution of spam and malware.
- 09.06. Unknown persons penetrate the systems of the British web hoster **VAserv** and manipulate or delete the data of more than 100,000 websites hosted here.
- 17.06. Around 2.2 million URLs of the URL shortening service **cli.gs** are manipulated and redirected to another target.
- 24.06. The Pentagon sets up a new **cyber warfare military command** under the orders of the US Defence Minister, which must be capable of countering warlike actions against the global security environment.



- 25.06. The Hanover department of public prosecution rules against the operators of the website **mega-downloads.net** due to massive fraud of computer users and freezes, in the course of investigations, company accounts to the tune of nearly one million euros. According to the estimates of consumer associations, nearly 20,000 computer per month were conned by hidden subscription fees.

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