



G Data

# Malware Report

## Semi-annual report July-December 2009

Ralf Benzmüller & Sabrina Berkenkopf  
G Data Security Labs

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

# Contents

<b>At a Glance</b> .....	<b>3</b>
<b>Malware: Facts and Figures</b> .....	<b>4</b>
Unlimited Growth? .....	4
Malware Categories.....	5
Multi-variant Families .....	6
Primary Target of Attack: Windows .....	8
<b>Outlook for 2010</b> .....	<b>9</b>
Outlook.....	9
<b>Web 2.0: Social Networks</b> .....	<b>10</b>
<b>Problem Case: Data Protection</b> .....	<b>13</b>
<b>Events and Trends in the Second Half of 2009</b> .....	<b>14</b>
July 2009 .....	14
August 2009 .....	14
September 2009 .....	15
October 2009 .....	16
November 2009 .....	16
December 2009 .....	18

## At a Glance

In the second half of 2009, 924,053 new types of malware were discovered. This is 39% higher than in the first half of the year and 60% up on the previous year's total, and hence a new record.

Throughout the whole of 2009 1,588,005 types of malware were discovered - 78% more than in 2008.

The proportion of Trojan horses has risen by 9.0%. With 42.6% they represent the largest part of the flood of malware.

Malware classified as worms, exploits and viruses has risen at an above-average rate.

The number of types of malware that use PDFs has almost tripled.

The volume of new adware has dropped by 25%.

Over the year as a whole 2,908 families emerged, against 3,069 in 2008. This means that the new record result can be traced back to fewer active malware families.

The most productive malware families are 'Genome' (3), 'PcClient' (new) and 'Hupigon' (1)<sup>1</sup>.

Windows is still the primary target for attacks, at 99.0%. A reduction of 0.3% over the first half of 2009 is accounted for by .NET malware (0.3%). Script languages for web applications maintain their share, at 0.5%.

## Forecast

Downloaders, backdoors and rootkits will retain their share. They have a solid place in the underground economy.

Exploits will also be put to use at lightning speed in the coming year.

Web applications are becoming ever more significant targets for attacks.

The significance of social networks such as MySpace, Facebook and Twitter as platforms for spam and sources of information for preparing and carrying out criminal activities will increase.

Data theft is and will remain a lucrative business. Banking trojans, spyware and keyloggers will retain their share.

## Events

Koobface is one year old and more active than ever.

Gumblar is the malware that infects the most web pages.

Numerous data leaks and data protection violations have shaken users' trust in the reliability of businesses, including in the credit card and banking sectors.

<sup>1</sup> Numbers in brackets refer to the position in the first half of 2009.

# Malware: Facts and Figures

## Unlimited Growth?

For years, the number of new types of malware has been growing continuously, as shown in Diagram 1. In the second half of 2009 once again, the number of new types of malware has risen to a new record level of 924,053.

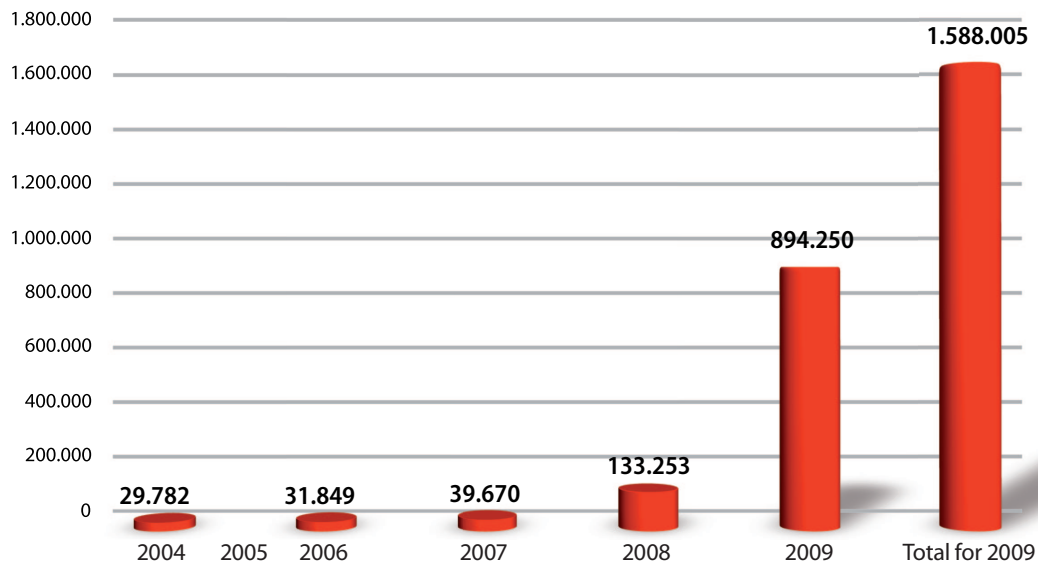


Diagram 1: Number of new types of malware per annum since 2004

The growth rate of 39% compared to the first half of 2009 and 60% compared to the same period last year is lower than the values in previous years. In 2009 as a whole, 1,588,005 types of malware were discovered - 78% more than in 2008. The number of new types of malware discovered in 2004 is now being matched in one week.

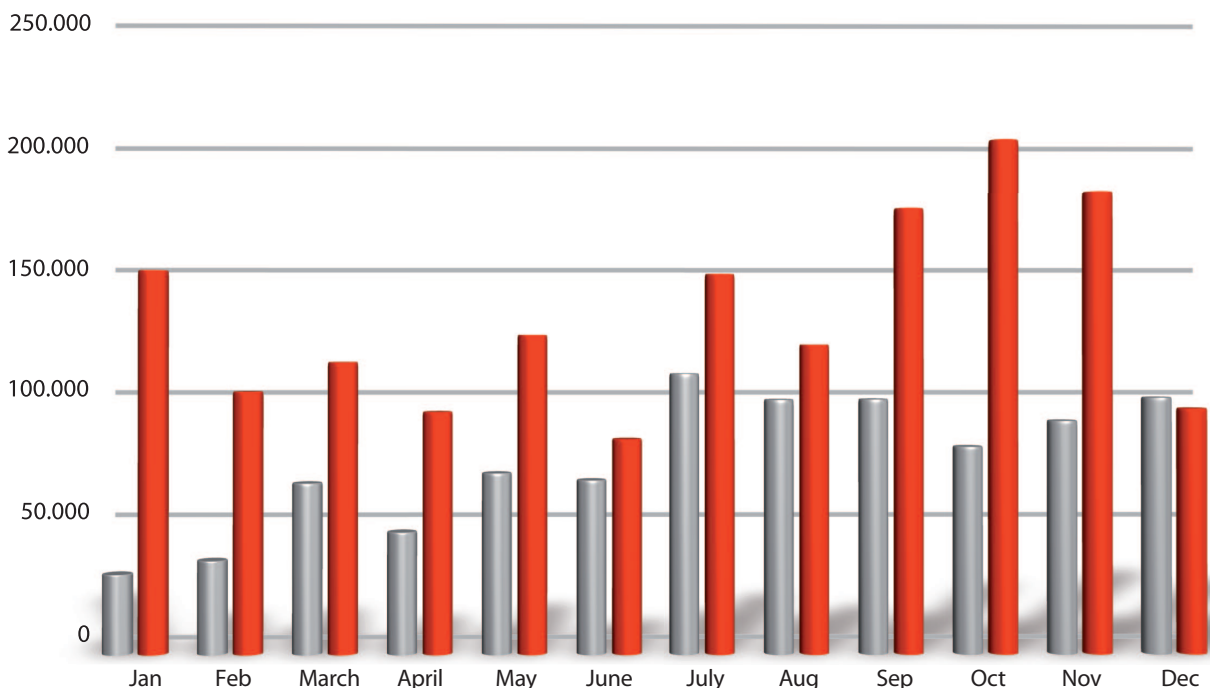


Diagram 2: Number of new types of malware per month for 2008 and 2009

## Malware Categories

The number of Trojan horses rose significantly in the second half of the year. Their proportion is - as Table 1 shows at 42.6% - 9.0% higher than in the first half of the year. Hence they are by far the most common category of malware. The number of downloaders, backdoors and tools is also growing. The figures are somewhat less than the average increase of 39% over the first half of the year and 60% over the same period last year. However, these categories represent the most significant elements of the black market in malware. Downloaders are used for distribution; backdoors enable computers to be controlled remotely (botnets); and tools are needed to give novices a way into the world of malware and to make everyday work easier for professionals.

Worms also recorded an above-average increase. Their number has almost doubled against the first half of the year and nearly tripled against the same period last year. The Basun family has contributed to this: it is the first worm for years to make it back into the Top 10. Autorun was the frontrunner among worms in the first half of the year.

The number of exploits has increased more than average. This is in contrast to the significant reduction in the number of security holes reported in CVE. At 4,594 weaknesses reported in 2009, this was significantly lower than the record level of 2008 where 7,250 weaknesses were recorded. The number of security holes discovered is therefore a poor reflection of the number of weaknesses being exploited by malware. And this number has increased significantly. Security holes in widely distributed software are being exploited more and more often, largely for attacking computers via the Internet. Computers with out-of-date software are soft targets for cybercriminals.

However, the category that recorded the biggest growth is one considered already dead - viruses. This category includes classic file infectors that attack executable files. The popularity of USB sticks and other removable data carriers lends itself to their use in such activities. However, with a share of 0.1%, its spread has been limited.

Category	# 2009 H2	Share	# 2009 H1	Share	Diff. 2009H2 2009H1	# 2008 H2	Share	Diff. 2009H2 2008H2
Trojan horses	393,421	42.6%	221,610	33.6%	+78	155,167	26.9%	+154
Downloaders/droppers	187,958	20.3%	147,942	22.1%	+27	115,358	20.0%	+63
Backdoors	137,484	14.9%	104,224	15.7%	+32	125,086	21.7%	+10
Spyware	86,410	9.4%	97,011	14.6%	-11	96,081	16.7%	-10
Worms	51,965	5.6%	26,542	4.0%	+96	17,504	3.0%	+197
Adware	30,572	3.3%	34,813	5.3%	-12	40,680	7.1%	-25
Tools	14,516	1.6%	11,413	1.6%	+27	7,727	1.3%	+88
Rootkits	11,720	1.3%	12,229	1.9%	-4	6,959	1.2%	+68
Exploits	3,412	0.4%	2,279	0.3%	+50	1,841	0.3%	+85
Viruses	637	0.1%	143	0.0%	+345	167	0.0%	+281
Diallers	415	0.0%	1,153	0.2%	-64	1,013	0.2%	-59
Miscellaneous	5,543	0.5%	4,593	0.7%	+21	8,419	1.5%	-34
Total	924,053	100.0%	663,952	100.0%	+39	576,002	100.0%	+60

Table 1: Number and percentage of new malware categories in the first and second halves of 2009 and their change

On the other hand, the number of new types of spyware has gone down. Their proportion has dropped to 9.4%, which is 5.2% less than in the first half of 2009 and 7.3% less than a year ago.

However, this does not mean that data is no longer being spied on. Quite the opposite. Spying functions are more frequently being integrated into more comprehensive packages that are classified as Trojan horses.

Rootkits are an important element for hiding spyware and backdoors. Their number has increased significantly in the first half of 2009 and their use in malware programs has since become firmly established. However the number of new rootkits has gone down slightly.

Against this, the area of adware has recorded a slackening-off. The number of new advertising malware is 25% less than the previous year's level. This can be mainly put down to the drop-off of Monder. In the last half year, Monder was the most productive malware family. In the second half of the year its productivity was significantly lower.

## Multi-variant Families

The functions and properties of computer malware enable them to be classified into families. In previous years the number of malware programs grew continually, whereas the number of families was steadily falling. In the first half of 2008 there were still 2,395, while in the second half, it was down to 2,094. In the first half of 2009, a total of 1,948 different examples of virus families were counted. In the second half of 2009 the number of malware families began to increase again. Malware from 2,200 different families were active during this period. Throughout the whole of 2009 there were 2,908 families as against 3,069 in 2008. Therefore the trend in concentration is continuing. As previously, the increasing number of computer malware is being generated by fewer and fewer families.

	# 2009 H2	Virus family	# 2009 H1	Virus family	# 2008 H2	Virus family
1	67,249	Genome	34,829	Monder	45,407	Hupigon
2	38,854	PcClient	26,879	Hupigon	35,361	OnlineGames
3	37,026	Hupigon	18,576	Genome	20,708	Monder
4	35,115	Scar	16,719	Buzus	18,718	MonderB
5	24,164	Buzus	16,675	OnlineGames	15,937	Cinmus
6	20,581	Lipler	13,889	Fraudload	13,133	Buzus
7	19,848	Magania	13,104	Bifrose	13,104	Magania
8	18,645	Refroso	11,106	Inject	12,805	PcClient
9	16,271	Sasfis	10,322	Poison	11,530	Zlob
10	16,225	Basun	10,312	Magania	10,412	Virtumonde

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

Table 2 shows the families that have generated the most variants in the last 18 months. The current frontrunner, Genome, produces an average 184 new variants every day. Backdoors such as PcClient and Hupigon in 2nd and 3rd places also produce over 100 variants per day on average.

### Genome

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

### PcClient

PcClient is a backdoor program that can be used for remotely controlling a computer and stealing data. It uses rootkit technology to hide its files and registry entries.

## **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.

## **Scar**

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

## **Buzus**

Trojan horses from 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.

## **Lipler**

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

## **Magania**

Trojan horses from the East Asian Magania family have specialised in the theft of gaming account data from the Taiwanese software producer Gamania. In general, copies of Magania are distributed via an email that contains a multi-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 uses a DLL to insert itself in Internet Explorer so that it can read the web traffic.

## **Refroso**

This Trojan horse is new to the Top 10. The first copies of it were discovered at the end of June 2009. It has backdoor functions and can attack other computers in a network.

## **Sasfis**

This Trojan horse installs a file on the computer and attempts to download additional ones from the Internet. These variants are often sent as email attachments.

## **Basun**

For the first time in two years, a worm has made its way back into the Top 10 of the most productive malware families. Basun copies itself onto the PC under the name of the current user or administrator. Then it attacks other computers in the local network to spread itself.

## Primary Target of Attack: Windows

Recent years have seen malware authors concentrating on the Windows platform. Just as it is absolutely evident that more and more malware is being developed, so too the proportion of malware for Windows is constantly increasing. In the past half year, this is slightly lower than the results for the last two half years, at 99.0% (see Table 3). However, this slight reduction is qualified by the malware for the third most popular platform. Malware produced in Microsoft Intermediate Language has significantly increased and its proportion has risen to 0.3%. MSIL is the intermediate format in which .NET applications present themselves in platform- and programming language-independent form. Malware authors are now also making increasing use of the benefits of the .NET environment. The majority of .NET applications are hosted on Windows.

Web page scripts (such as JavaScript, PHP, HTML, ASP etc.) are doggedly asserting their 0.5% proportion. Infected web pages are becoming ever more popular methods of infection. 3,295 of the 4,371 web scripts are JavaScript malware. But JavaScript is not just installed in web pages. 1,624 malware programs use PDFs as their distribution medium. In 2008 there were 780 malware programs based on PDF; in 2009 their number has increased to 2,394 - almost triple.

	Platform	# 2009 H2	Share	# 2009 H1	% 2009 H1	# 2008 H2	% 2008 H2
1	Win32	915,197	99.0%	659,009	99.3%	571,568	99.2%
2	WebScripts	4,371	0.5%	3,301	0.5%	2,961	0.5%
3	MSIL	2,732	0.3%	365	0.1%	318	0.1%
4	Scripts	1,124	0.1%	924	0.1%	1,062	0.2%
5	NSIS	229	0.0%	48	0.0%	58	0.0%
6	Mobile	120	0.0%	106	0.0%	70	0.0%

Table 3: Top 5 platforms in 2008 and 2009.

*WebScripts refer to malware that is based on JavaScript, HTML, Flash/Shockwave, PHP or ASP and that usually exploits weak points via the browser. Scripts are batch or shell scripts or programs that have been written in the VBS, Perl, Python or Ruby scripting languages. MSIL is malware stored in the byte code of .NET programmes. NSIS is the installation platform that is also used by Winamp. Mobile encompasses malware for J2ME, Symbian and Windows CE.*

Its significant increase has seen the NSIS platform edge the 120 malware programs for mobile platforms out of the Top 5. Despite isolated incidents, mobile malware is not asserting itself. NSIS is the installation platform that is used for installing the Winamp media player etc. The popularity of NSIS as an installation platform is not just based on legal software developers.

For Unix-based systems, 37 malware programs appeared (in comparison with 66 in the first half of 2009), while for Apple's OS X, only 8 new malware programs were found. Compared to the mass of malware for Windows, the proportions on other platforms are infinitesimally small.

## Outlook for 2010

The commercial use of malware is persisting. The immense turnover in the underground economy enables the development of new technologies for spreading, using and camouflaging malware to forge ahead. Investment in emergent usage areas such as social networking, mobile devices, games consoles and little-used operating systems also enables this to happen. If these efforts also prove to be lucrative, cybercriminals will surely redirect their activities. But there are no indications of this at the moment.

Hence the year ahead will not see any kind of ebb in the flood of malware - on the contrary, the opposite will happen. Downloaders, backdoors, tools and rootkits are a constant component of this black market and will use ever more refined methods to carry out their tasks.

In terms of exploits, security holes in popular desktop applications will continue to be put to use at lightning speed. The reduced number of security holes reported and the increased security knowledge that software developers have may lead to an explosion in web applications. The more popular leasing of software and its use on the Internet becomes, the more lucrative it is for cybercriminals to hijack leased web applications. The same applies with options for leased computers (keyword: cloud computing). It remains to be seen whether developers of web applications will demonstrate the same care when implementing security standards that they have now established for desktop software.

New operating systems and computer platforms have been announced for the coming year. We will have to wait to see how these markets respond to them. The number of malware programs on Apple, Unix and portable computers may increase. The slow move to 64-bit versions of Windows 7 will also necessitate a change for malware authors.

## Outlook

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

## Web 2.0: Social Networks

Over time the Internet has developed from a medium with an academic undertone to an everyday medium for the wider masses. One in four people now uses the Internet.<sup>2</sup> This number in itself is impressive enough. But if you also look at the user statistics for the world's largest social network community, Facebook, it is clear what proportion of Internet usage the online community now has: according to statements from Facebook founder Mark Zuckerberg, in December 2009 more than 350 million people<sup>3</sup> were on Facebook - which means by implication that, from a statistical point of view, one in five Internet users has a profile on the US Web 2.0 provider!

However, the wide range of Web 2.0 applications does not just consist of social networks: Google Docs, Google Maps, Picasa, Flickr, Identi.ca, Jaiku etc. are just a few additional examples of web sharing. And because the broad palette of Web 2.0 applications is so useful and appealing, each service hides its own dangers. This is manifested on the one hand in the way that users publish a lot - often too much - personal information about themselves on community pages, and on the other hand through the technical structure of the platforms. The framework is already open to attack by cybercriminals - as we see time and again in other cases - yet the networks implement more and more applications that each present a separate target.



### Market leader Facebook as an example

Being an example of the community, Facebook typically exposes users to a large number of attacks and inconveniences. Apart from the constant criticism of the network's privacy settings and inadequate protection of younger members, dangers for users lurk in various places:

In mid-November more than 200 Facebook groups were taken over and renamed by an initiative called 'Control Your Info'. The group wanted to use this apparently harmless activity to raise awareness of a security hole, making it possible to modify content in groups without even having to hack into Facebook. The 'Control Your Info' group simply had to register itself as the administrator of the groups - while excluding the actual administrator. Changing the names of the groups and the content ought to attract attention; however it can also damage the reputation of the unwitting user if the attacker e.g. posts illegal content. Administrators of groups can distribute messages to all the members in the group and thus spread spam etc.

<sup>2</sup> According to [www.internetworldstats.com](http://www.internetworldstats.com) there are 1,733,933,741 Internet users worldwide, corresponding to around 25% of the world population.

<sup>3</sup> Source: <http://blog.facebook.com/blog.php?post=190423927130>

## **Spam from your own circle of friends**

Messages sent by contacts from a Facebook address book or a Facebook group are seen as legitimate by the majority of users. However, if spam is sent from a hijacked group or via a friend's Facebook account after it has been taken over without their permission, checking is better than just trusting. Messages are sent promoting a funny video, shocking photos or just brand new, interesting content.

Attached to it is a link: by clicking on this, the computer can be infected in a number of different ways - an unnoticed drive-by download or a falsified and infected codec for viewing the funny video are the most popular tricks. Something that has been operating as a email scam for years has now also spread into social networks. Facebook users have already had frequent encounters with exactly this pseudo-trustworthiness trick.

## **Koobface in abundance**

For over a year the Koobface worm has been up to mischief in Web 2.0 portals, and in 2009 antivirus providers were holding their breath. The most recent example associated with US-based Facebook involves the circulation of a video called 'SantA'. Clicking on the video opens a web page with an apparently necessary codec. Installing this false codec loads Koobface onto the victim's computer; this then spreads itself onto all the victim's social networks that it can.

In the second half of the year, Koobface had already found numerous other new gateways into the world of social networks. Cancelling the captcha function when logging on, registering a new user with a full profile, distributing falsified video codecs for more new videos, and much more - it is always on the lookout for new data that the worm can read, store and distribute. As soon as the worm is integrated into a community member's circle of friends, it diligently goes about its work as a collator and distributes itself.

One variant was discovered in Skype. The Trojan distributed itself via infected web pages, stole Skype users' login data and read data from the Skype address book. Users of other large social networks (e.g. MySpace, Hi5) are also at risk.

## **Twitter also has the potential for attack**

Micro-blogging service Twitter is one of the most popular web applications for keeping in contact with fellow human beings. However, the desire to be able to tweet anywhere and any time also gives rise to new security holes. In August a Twitter account was used to control a botnet using Base64-encoded short messages. Twitter blocked the account immediately.

Another risk of infection, especially with the short message blog services, arises from short URLs. Users cannot see the real link behind the abbreviation and quickly fall victim to infected sites.

Recognised URL abbreviation services include TinyURL, bit.ly, is.gd, tr.im and twi.bz.

Users should not trust the abbreviated link or the reliability of the person who has published it; users can be lured into traps if Twitter accounts are being hijacked. Before clicking on a short URL, users should apply the security measures provided by the abbreviation services themselves to identify any potential risk. The services' own information pages on the corresponding short URL can be referred to.

Here are a few examples of recognised services and their information pages:

**<http://www.gdata.de/virenforschung/news.html>**

	Short URL	Action	URL preview option
TinyURL	<a href="http://tinyurl.com/yzuwcwd">http://tinyurl.com/yzuwcwd</a>	preview. before the URL	<a href="http://preview.tinyurl.com/yzuwcwd">http://preview.tinyurl.com/yzuwcwd</a>
bit.ly	<a href="http://bit.ly/7jH8xP">http://bit.ly/7jH8xP</a>	/info after bit.ly	<a href="http://bit.ly/info/7jH8xP">http://bit.ly/info/7jH8xP</a>
is.gd	<a href="http://is.gd/5yGtz">http://is.gd/5yGtz</a>	- after the URL	<a href="http://is.gd/5yGtz-">http://is.gd/5yGtz-</a>
twi.bz	<a href="http://gdata.de.twi.bz/b">http://gdata.de.twi.bz/b</a>	/e after the URL	<a href="http://gdata.de.twi.bz/b/e">http://gdata.de.twi.bz/b/e</a>
tr.im	<a href="http://tr.im/lqpj">http://tr.im/lqpj</a>	-	-

Table 4: Example of short URLs and their preview options

## Conclusion

The number of attacks on Web 2.0 applications will continue to increase. Data sets are and will continue to be highly interesting and profitable wares for black market dealers and identity thieves. New variants of malware that arose in 2009 will continue to spread, and malware authors will refine them to exploit more and more new weaknesses in portals and APIs.

## Problem Case: Data Protection

In the second half of 2009 an above-average number of problems was encountered in the area of data protection. The range of problems reported in this area is vast: it stretches from data theft and abuse to illegal monitoring. With data theft, the distinction must be made as to whether the data was lost because a security hole in a computer system or other electronic system was exploited by external attackers or whether the data removal occurred with inside help.

The biggest problem with data holes is that the data can be distributed uncontrollably once it is in circulation and cannot be retrieved. Those affected have almost no chance of stopping it from being copied.

A headline in November 2009 involved a data leak at a Spanish credit card service.

Apparently the hole was located at a Spanish card billing service provider. Consequently over 100,000 credit cards belonging mainly to German and British customers were renewed. Even though the number of cards renewed was just a small percentage of the total number, the vulnerability created by this incident was clear to see.

Credit card data can be stolen in numerous places:

- When making a payment, primed card reading devices copy data from the card.
- Data is captured from the PC by keyloggers and other spy programs e.g. when shopping online.
- On falsified websites (phishing) or in deceitful web shops offering 'bait', the data is requested in a form and entered by the victim.
- Inadequately protected databases from online shops, payment services and banks contain transaction data. These are repeatedly targeted by attempted attacks.



Credit card owners cannot control every aspect of the data processing. And we hear again and again of people falling victim to credit card criminals. Many users start to feel unsafe and consider abandoning their credit card, but that is no alternative.

Credit card holders can actively protect themselves against the risk from such attackers.

- Keep the operating system and browser fully up-to-date
- Install and keep up-to-date a reliable, comprehensive virus protection package
- When entering data on forms, always check whether the site operator actually needs the information being requested. Only supply PINs, TANs, passwords and credit card security codes (CCV) when paying for something
- Only send sensitive data via https (i.e. encrypted).

## Events and Trends in the Second Half of 2009

The second half of 2009 is marked by the impact of attacks on social networks. Whether Twitter, MySpace, Facebook or another service, the attraction to phishers and malware distributors is undiminished.

### July 2009

01-07 The "**Month of Twitter Bugs**" begins. Aviv Raff, who has been taking part in the "Month of Bugs" project since 2006, wanted to alert users and programmers to the weaknesses of Web 2.0. His current focus here is on vulnerable Twitter browser APIs, Tiny-URL services and images primed with worm malware.

04-07 US and South Korean computers under fire on **Independence Day**.

**Targeted DDoS attacks** keep security experts from both governments busy.

A botnet consisting of multiple thousands of zombie PCs attacks government and other websites of economic significance, e.g. the New York Stock Exchange and South Korean banks. Intelligence services suspect the attacks were launched by North Korea.

08-07 The **Milw0rm exploit portal** announces its closure. This is averted following intense discussions. Even though the reasons for this were not made clear, experts assume that the number of exploits being hosted exceeded the operator's capacity. The portal is a contact point for IT security researchers from both the 'light' as well as the 'dark' side.

09-07 **Strange but true: A South African bank** initiated **skimming counter-measures** at ATMs. In a routine check by a technician, the defence system set off an alarm and, with it, a **pepper spray attack**. Three technicians needed hospital treatment.



23-07 A previously **unknown security hole** in the authplay.dll component in **Adobe Acrobat** and **Adobe Flashplayer** is used by drive-by download in infected PDF files and manipulated websites.

### August 2009

**Koobface** is one year old and has not let up in its aggression.

04-08 The **BSI** distances itself from email allegedly sent by it that directs users to a **scareware** site. Here careless users are lured to a subscription site with a two-year contract costing 192 Euro.

06-08 Micro-blogging service **Twitter** is **down** for several hours. The main application and API clients are compromised. The cause was probably a combination of **distributed denial of service (DDoS)** and an apparently targeted offensive against a blogger called 'Cyxymu', using additional clicks in spam email that direct users to certain Twitter pages.

13-08 It was announced that **Microsoft** had known about a critical **Zero Day hole** for two years and first reacted to it on patch day in July 2007.

14-08 **Twitter** possibly abused as a **botnet communicator**: an Arbor Security researcher discovered encrypted Twitter entries in an account that contained potential commands for a botnet.



24-08 The Stockholm District Court sentenced Internet Service Provider **Black Internet** to block traffic to the website '**The Pirate Bay**' or pay a fine of 500,000 Swedish krone (ca. 48,000 Euro). Soon after 'The Pirate Bay' found another provider.

27-08 A former employee of a security firm publishes programming code for smuggling a **software bugging device into Skype**. The bug can silently record conversations and send them as MP3 files to a predefined address.

29-08 In **China four software pirates** are given a prison sentence and fined ca. \$1.6 million. They are charged with distributing illegal copies of Windows XP and other software.

## September 2009

04-09 **T-Online customers** sometimes have to wait for days for their email. Several customer PCs were infected and were operating as spam 'spray guns', linked into a **botnet**. The email service's slowdown is eliminated by disconnecting the zombie computers from the Internet.

08-09 **Strange but true**: a resourceful **Austrian man** logged the **unencrypted data traffic** between a control centre and fire, rescue and ambulance service action forces. In this way he obtained information regarding incident locations, patient data and details of the particular incident.

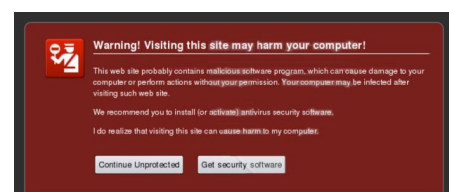
14-09 Visitors to the **New York Times website** fall victim to a **social engineering attack**. Hackers switched on scareware advertising banners on the homepage and urged unsuspecting visitors to download expensive, ineffective antivirus software.

15-09 Najat M'jid Maalla, a UN reporter, brings attention to a dramatic **increase in child pornography websites**. She explains that the number of mass exploitation sites has increased fourfold from 2003 to 2007. According to UNICEF estimates, there are over four million such websites in circulation.

16-09 **Strange but true**: a man in the USA gets his **two stolen laptops** back with the help of a **remote access** program. The man is able to watch the criminal surfing, chatting, writing email, video-chatting and visiting adults websites via RA and films his activities via a video camera. The **police** has no trouble finding him.

18-09 **Microsoft** sues companies that operate so-called **malvertising**. In probably the first case of its kind, Microsoft is leading the way against the spread of dubious advertising banners with embedded malware.

21-09 In systems infected with the Trojan.FakeAlert.BFW **Trojan horse**, the entire URL traffic is redirected to a falsified security warning. This warning imitates that in the Firefox browser and urges users to install 'Personal Antivirus' **scareware**.



Screenshot 1: The falsified security warning for the 'Personal Antivirus' scareware

## October 2009

- 01-10 **Crackers** have hacked into **Facebook's captcha** security request and can create profiles automatically. The profiles set up then use a link to entice users to go to a supposed video and attempt to convince the user to install fake antivirus software (rogueware).
- 02-10 **Google** removes the homepage of illegal swap shop '**The Pirate Bay**' and seven other sites that belong to the BitTorrent tracker website from its search results.
- 06-10 A list of tens of thousands of user names and associated passwords for Microsoft Live Hot-mail accounts appears on the Internet. The data was probably captured in **phishing attacks** and compiled into a list. Shortly after it is announced that Yahoo, Gmail, Comcast and Earthlink accounts have also been compromised.
- 07-10 **Strange but true: FBI head** Robert Mueller almost falls victim to a bank **phishing email**. In a statement, he says the email looked uncannily genuine and he followed the request to 'verify his data', until he 'clicked'. His wife has since banned him from online banking.
- 08-10 **FBI operation 'Phish Fry'** leads to accusations against 100 people in connection with phishing attacks. The phishers' system: Egyptian hackers detect victims' **personal and bank data** and forward this to American 'colleagues', who abuse the data for illegal financial transactions.
- 08-10 The six-month **De-Mail pilot project** is launched in Berlin. De-Mail is intended to enable legal documents in Germany to be exchanged as encrypted electronic 'shipping units'.
- 09-10 **Zombie computers** linked to the **Bahama botnet** divert search requests to clones made to look genuine instead of calling up the proper sites. Google, Bing and Yahoo search pages are especially compromised right now. The purpose of this is to earn money through click fraud.
- 17-10 The **netzpolitik.org** site receives a data set containing personal **data** of several hundreds of thousands of users of the German portal **schülerVZ**. The data was collected using a data collation program (crawler).
- 19-10 A Swedish court adjourns the **case** between members of the illegal P2P site '**The Pirate Bay**' and the entertainment industry to summer 2010. Two judges in the case are accused of bias. The case was originally due to begin on November 13 2009.
- 23-10 Click Forensics publishes a report showing that in the third quarter of 2009 42.6% of computer **click fraud** originated from botnets - an increase of 5.7%.
- 31-10 The 20-year-old man arrested two weeks before for capturing data from German language online community **schülerVZ** commits **suicide** in his cell.

## November 2009

- 01-11 The **Conficker worm** infects its **seven millionth victim** this week. Its combination of distribution, camouflage and protection mechanisms makes it the most successful malware program of the year.

03-11 A 20-year-old couple is arrested in Manchester. The pair are allegedly **distributors** of **Zbot spyware**. This steals online banking information, credit card data and passwords. It is the first arrest of this kind in Europe.

05-11 **Strange but true:** Macintosh computer vulnerable to 'malware program'. The malware program developed as an imitation of the game Space Invaders deletes a file from the Documents folder whenever an alien is shot in the game '**Lose/Lose**'. However the developer expressly informs the player of this before the game.



*Screenshot 2: Game view from 'Lose/Lose'*

10-11 The authors of **Koobface** succeed for the first time in programming a variant that behaves like a person in the social network Facebook. The malware program registers accounts, sets up a normal-looking profile, sends friendship invitations and even posts messages on other users' walls.

17-11 British telecoms subsidiary **T-Mobile** is embroiled in a data scandal. Employees sell data on thousands of customers to middlemen.

20-11 **Microsoft** pressurised to take action. Crackers post a **Zero Day exploit** for the Internet Explorer 5, 6 and 7 web browsers. The code is not actually harmful in all cases and on all computers, however crackers are working hard to improve the code.

24-11 Blow against **online crime**. More than 200 policemen from Germany and Austria carry out **raids** on 50 addresses and take four people into temporary custody. Those searched are suspected of exchanging and dealing in stolen credit card data, account data and malware. The 'elite crew' are said to be in control of a botnet with more than 100,000 computers.

24.11. In the USA the self-appointed '**Godfather of Spam**', 64-year-old Alan Ralsky, is **sentenced** to 51 months in prison, 5 years' suspended sentence and a \$250,000 fine. Together with his accomplices, who also get heavy sentences, he had been pushing out vast quantities of email spam.

25-11 **Strange but true:** South Korea restricts the sending of SMS. **South Korea's** struggle against **spam** has reached the mobile phone sector. Now only 500 **SMS** messages per mobile phone per day can be sent. Even though there are severe penalties for disseminating unsolicited messages in the republic, the flood of spam is extremely high. In terms of statistics, in October 98% of South Koreans possessed a mobile phone, representing 47.7 million devices.

27-11 A new **wave of spam** is afflicting **World of Warcraft players** in particular. An email with pictures of young Asian women urges recipients to click on a video attachment, which turns out to be a Trojan horse and spies on targeted WoW account data.

29-11 **Strange but true:** The '**Top Word of 2009**' in the English language is 'Twitter', according to the operators of website Global Language Monitor. 'Twitter' pushes the words 'Obama',

'H1N1', 'Stimulus' and 'Vampire' in 2nd to 5th places. The words of the decade were 'Global Warming', '9/11' and 'Obama'.

## December 2009

04-12 Users of **virtual hotel world Habbo** are facing an international wave of **phishing attacks**. Online criminals are trying to use phishing sites to gain access to players' access data and credit card data. Fraudulent blog entries are appearing en masse as well. Especially controversial is the fact that the online game is mainly aimed at children and adolescents.



*Screenshot 3: Users of the virtual Habbo hotel are lured into a trap by fraudsters*

06-12 German **children's portal** haefft.de is completely unsecured against data thieves, according to **Chaos Computer Club**. The CCC reports that you can move around in the community without having a password and with no technical manipulation, and thus acquire data. The site has been removed from the Internet.

08-12 'Crack WLAN encryption' service: a US company offers to use 400 cloud CPUs and **dictionary attacks** to bring down the **WPA encryption** of a radio network in 20 minutes. The cost: \$34.

15-12 A **previously unknown weakness** in the Doc.media.newPlayer function has been discovered in Adobe Reader and Adobe Acrobat 9.2 and older. In the worst case this hole enables an attacker to take over a compromised system. Adobe has announced a patch for January 12 2010.

16-12 A **pirate copier** of the film 'X-Men Origins: Wolverine' is arrested in New York after a nine-month search. The 47-year-old distributed the unfinished film in file sharing networks prior to its cinema release; however, he was not the actual source. There is still no information regarding who originally stole the film.

17-12 An attack on **Twitter** paralysed the homepage using **manipulated DNS entries** and displayed a page for the 'Iranian Cyber Army'. After the incident, Twitter operators suspect that it was an attack against Twitter as a provider rather than an attack against users. No other damage is known of.