G Data
Malware Report

Half-yearly report
January – June 2011

Ralf Benzmüller & Sabrina Berkenkopf
G Data SecurityLabs

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

Contents

At a Glance

- During the first half of 2011, 1,245,403 new computer malware programs were identified. This was 15.7% more than in the previous six months. The average number of new malware programs per day increased to 6,881.
- Among the different malware categories, Trojan horses and adware recorded above average growth. The number of backdoors and downloaders, in contrast, has declined slightly. Exploiting infected computers is clearly more important than recruiting new bots.
- In the first half of 2011 there were a total of 2,670 active malware families.
- The share of Windows malware increased to 99.6%. Classic Windows program files dropped 0.3% proportionately, but the increase in .NET programs compensated for this loss.
- Malware programs active on websites and malware for mobile devices show an upward trend.

Trends

- Hacktivism is becoming increasingly popular as a way of expressing political opinions.
- Malware for mobile devices is very much on the rise. The number of new threats is growing rapidly.

Events

- This year, close cooperation between Microsoft's Digital Crimes Unit and international police authorities successfully shut down botnet behemoth Rustock. March saw the successful deactivation of the computer network, which was responsible for generating billions of spam emails per day.
- Since April there has been a series of highly-reported cyber attacks on Japanese group Sony. These attacks mainly affected the Sony Playstation Network and its gamers. The hacker group presumed to be responsible for this, Anonymous, appeared numerous times over the following weeks along with LulzSec hackers.

Outlook for the second half of 2011

We expect the number of malware programs to increase again in the second half of the year. More than 2.5 million malware programs will be found this year.

In the second half of the year, cyber criminals will increasingly use mobile platforms, especially Android, for attacks.

Malware: Facts and Figures

The growth continues

The assumption that there would be hardly any increase in the flood of malware has proved false with regards to the first six months of this year. In the first half of 2011 the number[1] of new malware programs increased by 15.7% to 1,245,403. This corresponds to an average of 6,881 new malware programs per day. We expect the threshold of 2.5 million new samples to be exceeded by the end of the year. If growth continues, 2011 will have more new malware programs than 2006 to 2009 put together.

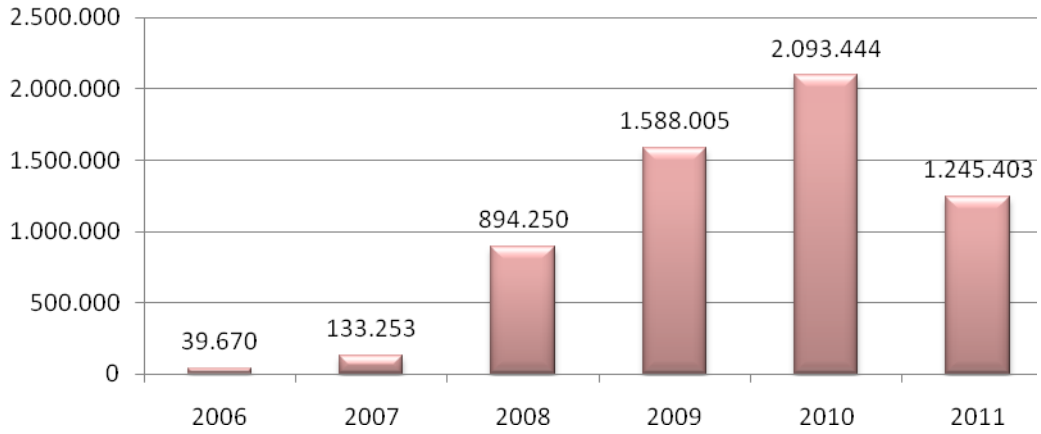


Diagram 1: *Number of new malware programs per year since 2006*

Malware categories

Malware is split into categories based on the degree of malicious activity. Diagram 2 shows the number of individual categories for the most recent half-yearly periods. The **Trojan horse** group recorded the sharpest increase in the first half of 2011. This group includes all malware that executes specific malicious functions. Most Trojan horses contain programs that are loaded onto infected computers via backdoors in order to carry out criminal activity. This group includes spamming, denial-of-service attacks, proxy services and similar offerings from the cyber crime economy's catalogue of services. The many variants of online banking Trojans ZeuS and SpyEye fall into this group as well. This growth shows underground business is going well.

The sharp increase in **adware** has slowed down somewhat since the second half of 2010. However, the 14.6% increase shows that adware continues to be a lucrative and little noticed business for the perpetrators.

[1]The figures in this report are based on the identification of malware using virus signatures. They are based on similarities in the code of harmful files. Much malware code is similar and is gathered together into families, in which minor deviations are referred to as variants. Fundamentally different files form the foundation form their own families. The count is based on new signature variants created in the first half of 2011.

There was a slight decrease in the number of **downloaders/droppers**, which are responsible for infecting computers. The number of **backdoors** also fell slightly. These malware programs make it possible to control computers remotely and integrate them into botnets. Clearly the establishment and management of botnets is no longer a priority. The number of **exploits** increased again slightly for the first time after a long decline.

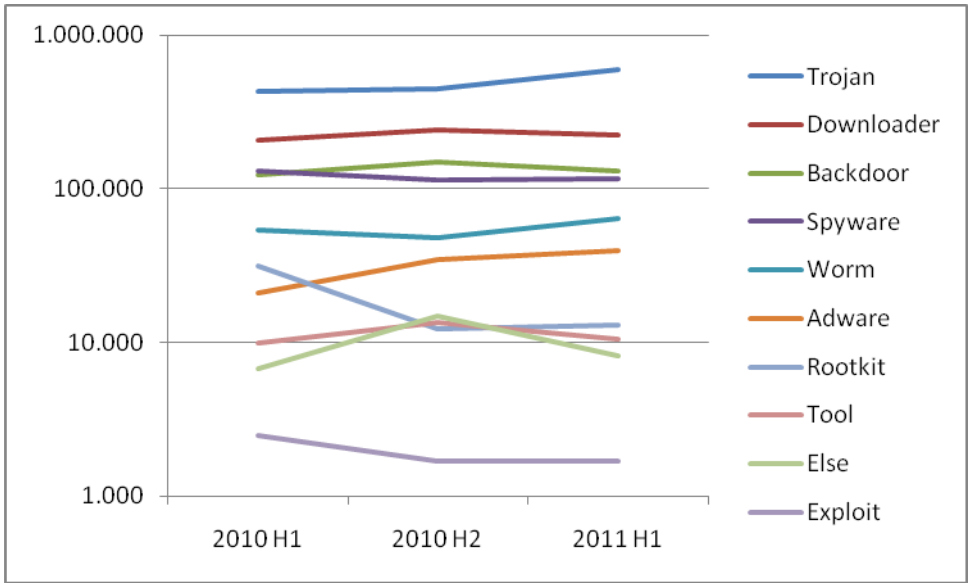
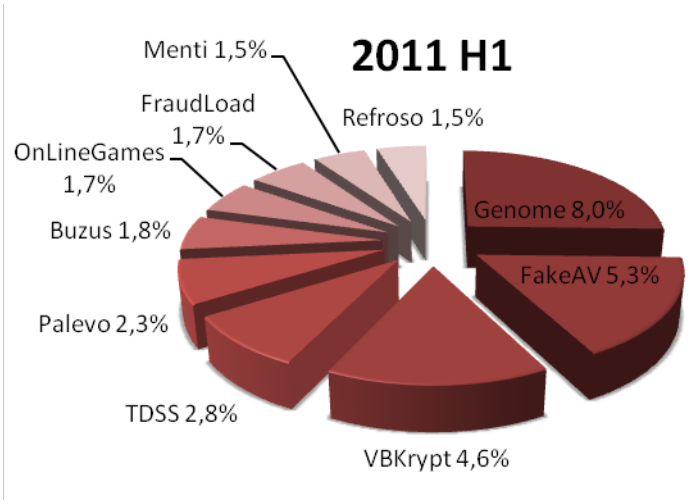


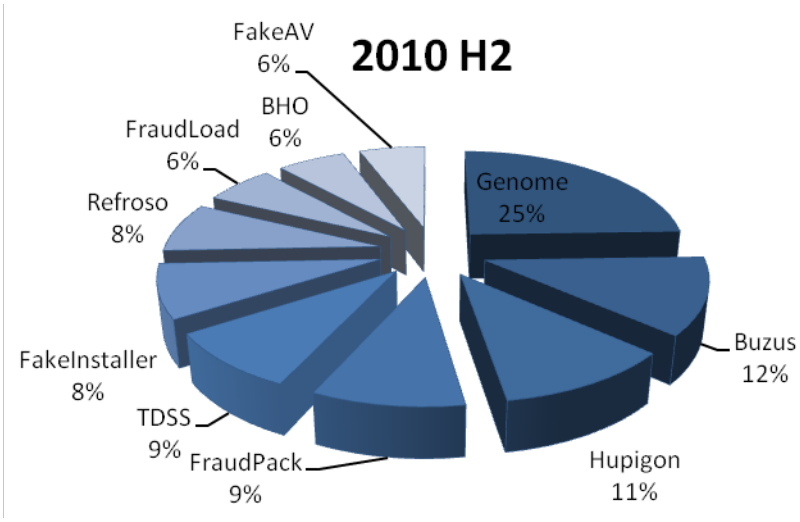
Diagram 2: *Number of new malware programs per category in the last three half-year periods*

Malware families

Malware is grouped into families based on properties and activities. Some families are very active and constantly produce new variants. Diagram 3 shows the most prolific families in recent half-year periods. The total number of malware families increased slightly by 2.4% to 2,670 in the first half of 2011.

Once again, first place goes to Genome, a Trojan horse with numerous malicious functions. In second place is FakeAV, a representative of a category of software that imitates virus protection or system tools that is very popular among cyber criminals. With VBKrypt, a new program for camouflaging malicious files has made it into the top 10. TDSS family rootkits - also known as TDL rootkits - reinforced their market-leading position in the cyber crime economy with a fourth, even more powerful version. The sharp increase in worms of the Palevo family is responsible for the significant increase in worms. The second last position is reserved for a newcomer. Menti is a Trojan horse, like first-placed Genome. This shows that Trojans continue to be the most popular malware used by perpetrators.





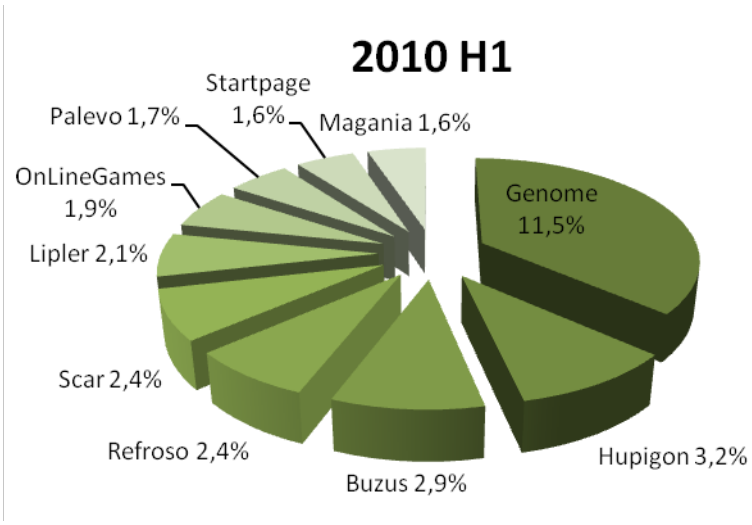


Diagram 3a-c: Top 10 most active malware families. Proportion of new variants 2010 and 2011

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

FakeAV
This Trojan horse pretends to be antivirus software 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.

VBKrypt
VBKrypt is a tool used to disguise malicious files. The camouflage routines are written in Visual Basic. The contents of the disguised files are very diverse and range from downloaders and backdoors to spyware and worms.

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.

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

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.

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

FraudLoad
The Fraudload family comprises numerous variants of so-called scareware programs, which present themselves to users as security software or system tools. The victim is led to believe that the system is being scanned for possible infections. To clear these supposed 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 users are lured to websites claiming to offer videos with erotic content or the latest news or gossip. To view the supposed videos, the victim is supposed to install a special video codec, which contains the malware.

Menti
Trojan horse Menti embeds itself in a compromised system and makes regular contact with a server. This computer thus becomes part of a botnet.

Refroso
This Trojan first appeared at the end of June 2009. It has backdoor functions and can attack other computers in a network.

Platforms

In the first half of 2011, the lion share of malware was once again written for Windows systems. Only one in two hundred and fifty malware programs is not a Windows program file[2]. The proportion of classic Windows program files (Win32) continues to drop. However, .NET programs (MSIL) compensate for this loss of 0.3% and the overall share of Windows malware programs is on the rise.

	Platform	# 2011 H1	Share	# 2010 H2	Share	Diff. 2011H1 2010H2	# 2010 H1	Share	Diff. 2011H1 2010H1
1	Win32	1.218.138	97,8 %	1.056.304	98,1 %	+15,3 %	1.001.902	98,5 %	+21,6 %
2	MSIL	21.736	1,7 %	15.475	1,4 %	+40,5 %	9.383	0,9 %	+131,7 %
3	WebScripts	3.123	0,3 %	2.237	0,2 %	+39,6 %	3.942	0,4 %	-20,8 %
4	Scripts[3]	832	0,1 %	1.111	0,1 %	-25,1 %	922	0,1 %	-9,8 %
5	Mobile	803	0,1 %	55	<0,1 %	+138,2 %	212	<0,1 %	+273,1 %
6	Java	313	<0,1 %	517	<0,1 %	-39,5 %	225	<0,1 %	+39,1 %
7	*ix[4]	233	<0,1 %	382	<0,1 %	-39,0 %	226	<0,1 %	+3,1 %
8	NSIS[5]	131	<0,1 %	130	<0,1 %	+0,8 %	260	<0,1 %	-49,6 %

Table1: *Top 8 platforms in the last three half-year periods*

The remaining 0.5% are dominated by web-based malicious code and have significantly increased in numbers. On the other hand, the number of script-based malware programs has decreased.

Malware for mobile devices also recorded a significant increase. The type of malicious functions indicates commercial use. Approximately two out of three smartphone malware programs send SMS to expensive phone numbers. Spyware and backdoors have also increased significantly. Cyber criminals are currently establishing a new scope of application here, which G Data SecurityLabs will be keeping an eye on in the coming months.

[2] If you combine the program files for Windows 32-bit and 64-bit systems and .NET programs (MSIL).
[3] "Scripts" are batch or shell scripts or programs that have been written in the VBS, Perl, Python or Ruby scripting languages.
[4] *ix stands for all Unix derivatives, e.g. Linux, FreeBSD, Solaris etc.
[5] NSIS is the installation platform used for installing the Winamp media player etc.

Trends for 2011

The following table depicts the changes we expect in the individual categories of malware and platforms.

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

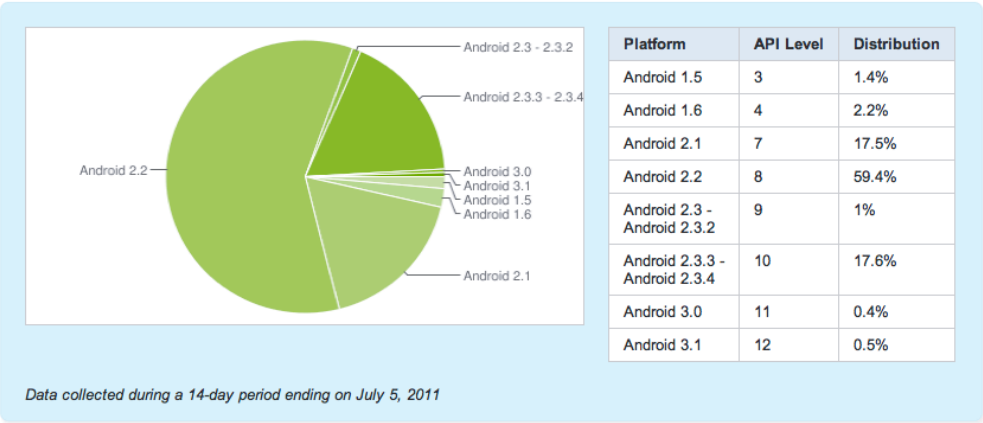
Table 2: *Anticipated development of malware categories and platforms*

Mobile Malware

Mobile devices with Android operating systems are becoming increasingly popular. For this reason, IDC market researchers are labelling Android as a future 'king of the hill'. However, this rise in popularity is accompanied by increasing interest on the part of malware authors in the platform and mobile media. Hence G Data is seeing an increasing tendency towards a high risk potential for mobile terminal devices. The continued development of mobile malware is expected to be faster than the development of malware for PCs, as established exploitation structures already exist in the underground.

The discovery of malware-infected apps on the Google Android Market has already made headlines in the media. Meanwhile, feature phones and smartphones continue to enjoy ever-increasing popularity among users worldwide.However, feature phones and smartphones are enjoying greater and greater popularity worldwide. They are increasingly used as a medium for payment services and are thus becoming ever more attractive to criminals. In some countries, they can anonymously sign up for expensive premium SMS numbers and thus incur large phone bills from SMS subscriptions for victims. Cyber criminals have once again extensively exploited these new opportunities: more than two thirds of all mobile malware sends SMS to expensive premium services. The number of backdoors that are used to integrate smartphones into botnets is also increasing dramatically. A specialised online banking Trojan that attacks the mTAN process has emerged in the form of Zeus in the Mobile (ZITMO). Sending TAN via SMS was originally intended to provide additional security through use of channel separation. As ZITMO intercepts the SMS with the TAN, the procedure is no longer secure. One thing is clear: mobile malware has moved on from the proof-of-concept phase.

The Android platform is continuing to gain popularity among customers, as devices with Android operating systems are cheaper than, for example, competitors using iOS. Furthermore, Android has a bigger range of devices from numerous telecommunications company brands. However, this range has the distinct disadvantage that it significantly complicates internal quality control and that it is not always possible to distribute updates to every customer in a timely manner. The devices from the competitor based in Cupertino, USA, provide an example of this. Furthermore, it is often not possible to upgrade older models of telephones. At the beginning of July, for example, the proportion of users visiting the Android Market with an old Android OS version was still very high (see figure 1). The long delivery path for new operating system versions - from Google to device manufacturers, via service providers to customers - gives villains the opportunity to exploit vulnerabilities in older operating systems in the meantime. These are delays of months, not days. This weakness will continue to be a focus for cyber criminals in the future.



Platform	API Level	Distribution
Android 1.5	3	1.4%
Android 1.6	4	2.2%
Android 2.1	7	17.5%
Android 2.2	8	59.4%
Android 2.3 - Android 2.3.2	9	1%
Android 2.3.3 - Android 2.3.4	10	17.6%
Android 3.0	11	0.4%
Android 3.1	12	0.5%

Data collected during a 14-day period ending on July 5, 2011

Figure 1: *Distribution of Android platforms among visitors to the Android Market (Source: http://developer.android.com/resources/dashboard/platform-versions.html)*

Besides the hardware-related risks, the 'human factor' should not be underestimated: During installation, users often confirm the displayed required authorisations without paying any attention. This opens the way for applications to gather information, call premium numbers and much more. Examples of this are the applications manipulated by Zsone on the Google Android Market. Unnoticed by the users, the apps send subscription registrations to premium SMS numbers in China and even intercept the response SMS from the subscription service. Users remain unaware of the expensive text messages - until they receive their phone bills. This malware currently only poses a threat to Android users in Chinese telecommunication networks.

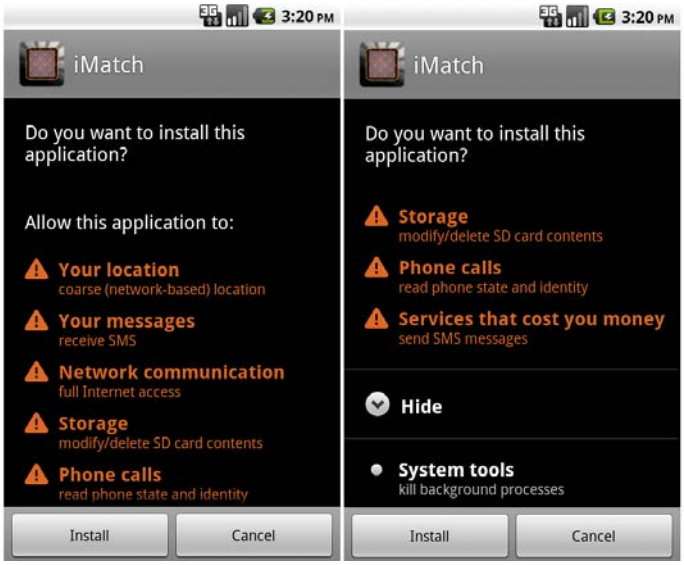


Figure 2: *An app infected by Zsone grants itself numerous authorisations on a mobile phone, enabling it to harm the user.*
(Source: G Data Software)

Conclusion

Cyber criminals are increasingly targeting mobile devices. The rate of malware development will therefore accelerate as there is more profit to be made by the attackers. The rising sales figures for Android devices make this market ever more appealing to the underground. Furthermore, since the opportunities for exploiting smartphones are far from being exhausted, increasing numbers of new technologies are providing more and more attack vectors - one example for the near future being payment with a smartphone via NFC (implemented in Android since version 2.3).

Events during the first half of 2011

January 2011

09.01. Australian media company Fairfax accuses **Vodafone** of inadequately securing its customer data in databases, making it visible to many - including all Vodafone dealers. Hence personal data such as **SMS and call logs** could also be seen by third parties, who apparently gained access to the data through a type of "pay per view" process. The revelation is labelled as an aftermath of the Wikileaks "Cablegate" affair.

11.01. The North Korean government's **Twitter and YouTube accounts** are hacked and abused by unknown persons. On the birthday of Kim Jong-un, the designated successor to Kim Jong-il, hackers use the accounts to broadcast **messages critical of the regime**. Furthermore the intruders publish an animated video showing him in a sports car, running over needy people. Members of South Korean Internet forum DC Inside claim responsibility for the hack.

Screenshot 1: *An animated video showing Kim Jong-un (Source: YouTube.com)*

16.01. The **Federal Criminal Police Office** (Bundeskriminalamt - BKA) arrests a Bulgarian **skimming gang** that had been manipulating ATMs in Dresden. The three men are caught red-handed in a bank branch as they are working on their equipment. Their total takings are unknown.

23.01. The Facebook accounts of French President **Nicolas Sarkozy** and Facebook CEO **Mark Zuckerberg** are compromised. The intruders publish deceptively real-looking comments on both pages in the names of the celebrities. How the perpetrators gained write access remains unclear.

24.01. Iran announces a **cyber police** force designed to prevent e.g. communication between political dissidents, primarily via social networks. Referring to protests against the re-election of President Ahmadinejad in 2009, police chief Esmaeil Ahmadi Moghaddam explains: "Through social networks in our country, **anti-revolutionary groups and dissidents** found each other and contacted foreign countries and incited unrest."

31.01. **Strange but true:** A **stolen laptop** belonging to a 25-year-old American woman automatically reports itself via email and thus facilitates police investigations in Newport, Virginia. **The device takes pictures** using the integrated webcam and sends them to the owner. Now the police just need to identify the two people in the published picture to find out how they came to be in possession of the laptop.

Screenshot 2: *Photo from the webcam of the stolen notebook (Source: wavy.com)*

February 2011

05.02. Aaron Barr, an employee of security firm **HBGary Federal**, exposes his company to a widespread, multi-level attack by the group Anonymous. He had previously boasted that he had identified the members of the **hacktivist group** that had carried out Operation Payback shortly before. Even the New York Times reported it and the publicity prompted the accused to strike back. Subsequently, exploiting a range of errors that should not occur in a security company, Anonymous got hold of passwords for HBGary employees and ultimately the Google mail account of Greg Hoglund, the company's co-founder and head of technology. Besides controversial information concerning armaments orders, it also contained access data for Hoglund's site **rootkit.com**. Anonymous published the data available there along with Hoglund's emails. Aaron Barr's big pitch ultimately led to his resignation.

07.02. Police authorities in Hamburg arrest two alleged operators of **subscription trap websites**. Since the end of 2008 the two had cheated over 65,000 website visitors and gained almost € 5 million in the process. The fraudsters basically offered free software - or at least software available as a free test version - for downloading and then signed visitors up to subscription contracts without their knowledge.

09.02. A toolkit called **Tinie App** can be bought on the underground market for around USD 25, making it possible for almost anyone to create their own **malicious application for Facebook**, for example, Profile Creeps or Creeper Tracker. Many users still click on such apps in Facebook and thus distribute them even wider - to the joy of the developers, who rake in money for the clicks via affiliate programs.

12.02. The **American Attorney General's Office and Department of Homeland Security** have erroneously applied a banner to 84,000 domains, listing swingeing penalties for anyone associated with **child pornography**. Due to a data transmission error, every domain of the FreeDNS DNS provider redirects to the banner, thus unsettling owners of and visitors to the websites.

Screenshot 3: The banner misleadingly displayed on 84,000 domains (Source: torrentfreak.com)

13.02. **Customer data** belonging to millions of users of services such as Pixmania, Eidos, eHarmony and diversitybusiness is **traded on the underground market**. Some data sets are offered there for prices between USD 2000 and 3000 (approx. EUR 1400 to 2100). Argentinean Chris Russo is potentially responsible for the data theft. In the case of eHarmony, the data was stolen by exploiting an **SQL injection vulnerability**.

15.02. Malicious code is injected into the **BBC 6 Music website** and the website for BBC Radio 1xtra as a consequence of a **mass infection of vulnerable websites**. The code downloaded files from a website and tries to infect website visitors without them

knowing (**drive-by infection**). The attackers use a Phoenix exploit kit to exploit vulnerabilities on the computer.

17.02. Research shows that **cyber crime** alone causes the **United Kingdom** GBP 27 billion (EUR 30.7 billion) in damages per year. Intellectual property theft makes up the largest portion of criminal activity here, followed by industrial espionage and blackmail.

28.02. **Strange but true:** A 48-year-old man from Naperville, Illinois falls victim to a **fraudulent online friendship**. In two years he sent the woman a total of **USD 200,000** (approx. EUR 139,000) to accounts in Britain, the USA, Malaysia and even Nigeria. When she stopped communicating with him, he became concerned that she may have been abducted and called the police. They then explained to him that he had been duped. Even the driver's licence that the woman had sent at one point was fake. It was a **sample ID** from the state of Florida.

March 2011

05.03. Google officially declares that a number of apps were removed from the **Android Market** on the previous Tuesday. The applications were infected with the **DroidDream** malware, which, among other things, tries to obtain root rights on compromised mobile devices. Google used remote access to uninstall the malicious programs on affected devices. The company also releases an “Android Market Security Tool March 2011”. A short time later, however, a **trojanised version** also appears on the market.

Screenshot 4: *Android Robot (Source: android.com)*

06.03. During an attack on the Egyptian state security service centre, government opponents find documents from British company Gamma International offering to sell a **spyware program called FinFisher** to the government. The malware is designed for spying, tapping and gaining control of dissidents' computers and was said to cost USD 525,000 (approx. EUR 364,000) including training.

16.03. About a year after shutting down the Waledac botnet, Microsoft reports another **successful botnet deactivation**: one of the biggest botnets in the world, called **Rustock**. The Microsoft Digital Crimes Unit (DCU) estimates that around one million computers had been infected with Rustock malware and that the botnet might have been responsible for billions of spam emails every day.

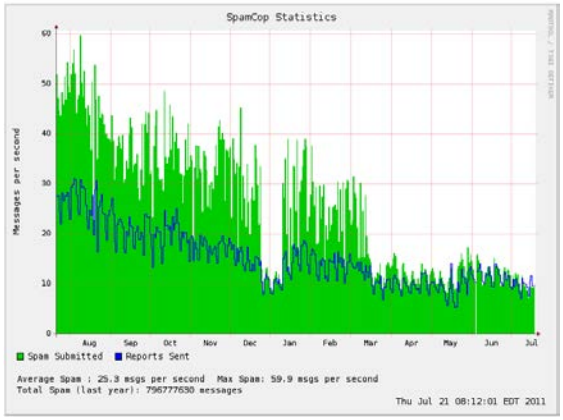


Figure 3: *This graph shows a significant reduction in the number of messages per second since mid-March (Source:*

17.03. Attackers hit **security company RSA**'s server and steal data on **SecurID** two-factor authentication. The attack, labelled an Advanced Persistent Threat, was executed systematically, using **manipulated Excel files** that were emailed to a small group of RSA employees. When the .xls files are opened, the malware exploits a Zero-Day vulnerability to gain access to privileged user accounts.

18.03. 29-year-old Ashley Mitchell is sentenced to two years in prison for stealing **400 billion virtual poker chips** worth USD 12 million (approx. EUR 8.4 million) from American company **Zynga**. Among others, Zynga operates the world famous online game Farmville. Mitchell sold part of his booty on the **black market** for GBP 53,000 (approx. EUR 60,000).

20.03. The **TripAdvisor** platform falls victim to data theft. Criminals attack the popular travel website and steal **members' email addresses** from a database. TripAdvisor closes the hole immediately and presumes that no major damage has been done. "You might receive spam email as a result of the incident," it says in an email to members.

23.03. Unknown attackers gain access to **SLL certificates** for existing websites by using a compromised account to infiltrate Comodo's Certificate Authority (CA). The certificates were stolen on March 15th and could be used to replicate real looking websites. **Comodo** states in a report that "the attacks came from multiple IPs, but mainly from Iran."

April 2011

04.04. Details of a large-scale **mass SQL injection attack** become known. The attack, known as the **Lizamoon attack**, smuggled malicious code into millions of websites. Cleaning up the affected sites is a longwinded affair. The malware redirected visitors from the actual websites to **FakeAV websites**, where fraudsters tried to make money.

08.04. **Strange but true:** A software company places a job advertisement for **female programmers and sales assistants**. The job requirements are that applicants must be between 20 and 39 years old and be prepared to work completely naked. The 63-year-old advertiser was promising genuine jobs with a genuine company.

20.04. In future the **American Department of Homeland Security** is planning to publish its **national terror alerts** not just on its own homepage, on TV and on the radio, but also on social networks such as **Facebook and Twitter**. Announcements in airports and notices on government websites would then be dropped.

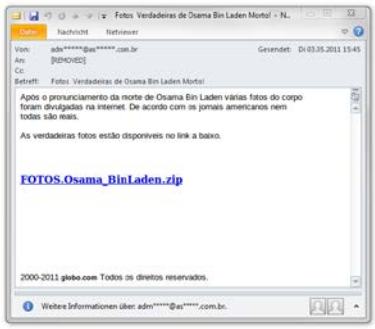
24.4. The 20-year-old son of security software manufacturer **Eugene Kaspersky** is safely released from the clutches of five kidnappers by Russian security authorities. He stated that **no ransom** had been paid. The kidnappers had demanded EUR 3 million.

27.4. The first Sony PlayStation customer **sues Sony Corp** for inadequately protecting personal data. Between April 17th and 19th hackers had attacked the Sony PlayStationNetwork (PSN) and the Qriocity online service and stolen **77 million sets of user data**.

May 2011

10.05. Finnish police break up a gang of **online banking fraudsters** and arrest 17 suspects. Customers of Finnish Nordea Bank were being targeted by the criminals who **stole approx. EUR 1.2 million** in over 100 rigged transactions. All but EUR 178,000 of the money was successfully restored to its rightful owners.

11.05. The announcement of the **death of Osama Bin Laden** inspires malware authors to use the distribution of supposed evidence photos, for example, to lure users into traps. The conspicuous **attack vectors** in this case are emails containing links to malware and primed Word documents that were supposed to exploit a vulnerability (CVE-2010-3333).



***Screenshot 5**: Dangerous Osama Bin Laden email.*

11.05. The website of Russian media agency **Pravda** is hacked and attacks users without their knowing. The criminals use **embedded exploit scripts** that attack a vulnerable version of Java on website visitors' computers. The attackers did not make any visual changes to the website, which made it considerably more dangerous.

20.05. Independent software researcher Rosario unveils an **exploit for Microsoft Internet Explorer** giving attackers access to websites that require a login, such as Facebook. After entering the login data, the website generates a cookie as a digital key. If this **cookie is stolen**, third parties can also gain access to websites that are supposed to be protected. The attack is known as "**cookiejacking**".

23.05. The complete **source code** for banking Trojan **ZeuS** is published. ZeuS has indisputably been the most powerful banking Trojan in recent years.

25.05. A PhD student at the University of Amsterdam loads **35 million Google Profiles data records** onto a database. This includes names, email addresses and biographical information. Collecting the information was intended to be an experiment to see how quickly private detectives and phishers, for example, could procure personal data in a targeted manner. Google does not prevent the lists from being indexed.

26.05. The **Chinese military** confirms for the first time that there is an **elite unit of cyber warriors** in its army. The special forces are known as the "Cyber Blue Team". It is not known whether the unit is purely defensive or whether it could be an offensive force.

June 2011

03.06. Following the attacks on **Sony PSN and Qriocity**, the **Sony Pictures** platform is now hacked. A group called **Lulz Security, or LulzSec for short**, claims responsibility for the attack. They stated that they stole personal data on more than 1 million users.

04.06. **Microsoft's DCU** continues to work on exposing the people behind the **Rustock botnet** disabled in March. The DCU presumes that the **controllers** were operating, or are still operating, from **Russia**. Hence they placed large advertisements in popular

Russian newspapers for 30 days to communicate with the owners of deactivated IP addresses and domains.

07.06. Arms manufacturer **Lockheed Martin** announces that an attack recently took place on its website that was facilitated by the **RSA SecurID tokens** stolen in March. Theft of data is said to have been prevented by quick intervention. They are currently in the process of renewing 45,000 SecurID tokens.

20.06. Virtual currency **Bitcoin** experiences a **slump in prices** on the Mt Gox trading platform. An unknown person hacked into a capital Bitcoin account (7.7% of all Bitcoins), converted the virtual money into US dollars and then back again. The price dropped from USD 17.50 per Bitcoin to one cent per Bitcoin.

26.06. After just 50 days, the **LulzSec** hacker group announces its breakup. The group, which is being hunted by police, has been responsible for numerous hacker attacks and denial of service attacks on websites in recent weeks. LulzSec published numerous captured data sets on the Internet. Experts consider LulzSec to be an offshoot of the Anonymous group.

29.06. Social network **MySpace** is sold. **Media mogul Rupert Murdoch** had purchased the platform for USD 580 million (approx. EUR 403 million) in 2005 and has now sold it at a huge loss to a Californian advertising company for **USD 35 million** (approx. EUR 24 million). Numbers of MySpace users dropped with the emergence of Facebook.

30.06. The German Federal Criminal Police Office (BKA) publishes **criminal statistics for Germany** for 2010: In the past year, 250,000 incidents of Internet crime were recorded. Compared to 2009, this represents an increase in such offences of around **20 percent**. The total damages incurred amount to EUR 61.5 million.