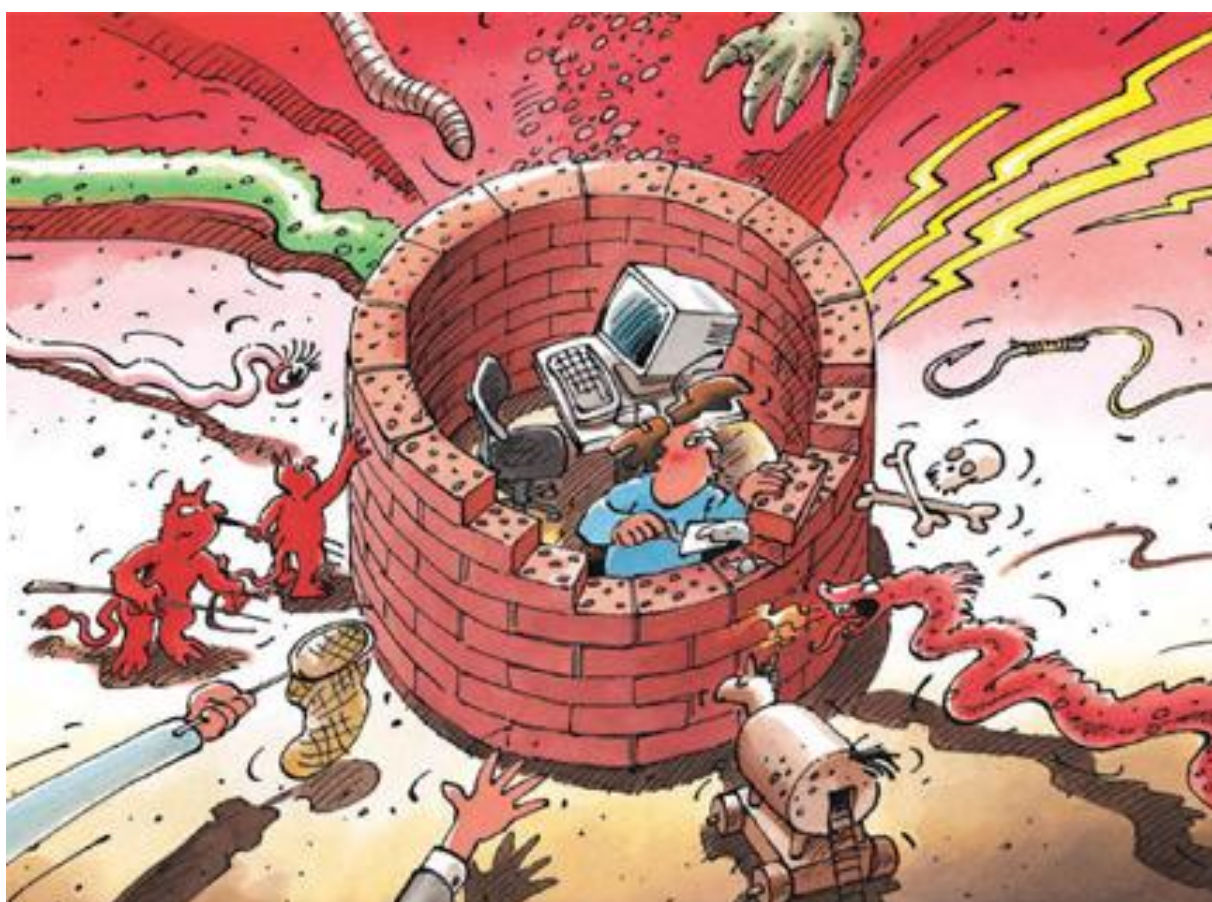




Information Assurance

Situation in Switzerland and Internationally

Semi-annual report 2009/I (January – June)



Contents

1	Focus Areas of Issue 2009/I	3
2	Introduction	4
3	Current National ICT Infrastructure Situation	5
3.1	Gozi – new Trojan spread via spam e-mails	5
3.2	Drive-by infections on the rise	6
3.3	Misuse of Swiss e-mail accounts	8
3.4	Interrupt of Cablecom Internet and telephone network	8
3.5	E-mails with malicious software targeted at major companies	9
4	Current International ICT Infrastructure Situation	10
4.1	IT espionage against Tibetan NGOs and the office of the Dalai Lama	10
4.2	Conficker	10
4.3	SCADA	12
4.4	Increased focus on military units for information warfare in various countries	14
4.5	More politically motivated DDoS attacks	15
4.6	T-Mobile network failure	16
4.7	UK: BBC acquires botnet for demonstration purposes	16
4.8	US: Massive increase of data mishaps in 2008	17
4.9	US wants to strengthen measures against cyber threats and improve protection	18
4.10	EU Commission wants to improve protection of critical infrastructures	18
4.11	Facebook changes its terms of service – for a short time	19
5	Trends / Outlook	20
5.1	Cloud computing, outsourcing, centralization, and information ownership	20
5.2	SCADA	21
5.3	General cybercrime developments	21
5.4	Drive-by infections	23
6	Glossary	23
7	Annex	28
7.1	ICANN and OFCOM are looking for solutions in combating fast flux networks	28
7.2	Browser settings for the protection against common Drive-by infections	33

1 Focus Areas of Issue 2009/I

- **Drive-by infections on the rise**

As already indicated in the last semi-annual reports, a shift of attack vectors (from e-mails with attachments or links) to website infections – so-called drive-by infections – is taking place. The classic ways of spreading malware apparently are no longer working so well, now that users are reacting more sensitively and opening strange-looking attachments less frequently. According to information by the security firm Scansafe, 74% of malware in the third quarter of 2008 was distributed via websites.

 - ▶ Current situation in Switzerland: [Chapter 3.2](#)
 - ▶ [Trends 5.4](#)
 - ▶ Defensive measures [Appendix 7.2](#)

- **Increasingly widespread discussion on security of SCADA systems**

Supervision, control, and data acquisition for industrial facilities, utilities for distributing vital goods (electricity, water, fuel, etc.), and transport and traffic systems (railways, traffic management systems, postal services, etc.) have long been unthinkable without information and communication technology (ICT). The development and operation of such supervisory control and data acquisition (SCADA) systems has a long tradition. The debate on the security of SCADA systems is thus becoming increasingly widespread. It is clear that such systems are key to the smooth functioning of our society. Dangers not only emanate from hacker attacks (sabotage), however, but also from technical failures.

 - ▶ Current situation in Switzerland: [Chapter 4.3](#)
 - ▶ [Trends 5.2](#)

- **Cloud computing and information ownership:**

On 17 May 2009, Swiss voters approved the introduction of biometric passports by a razor-thin majority of 50.1%. Along with concerns relating to data protection, an argument arising from the field of information assurance appeared to be partially responsible for the tight outcome.

 - ▶ [Trends 5.1](#)

- **Advance payment scam and subscription trap**

MELANI and CYCO still receive daily reports on a wide range of incidents relating to advance payment scams, supposed lottery winnings, and free offers. Apparently, this kind of Internet crime is still too successful.

 - ▶ [Trends 5.2](#)

- **Conficker**

The computer worm Conficker was one of the main IT topics in the media in the last half year. Especially around 1 April 2009, the date on which the worm was expected to update itself, media interest was enormous. No one actually had still been expecting such a worm outbreak, but Conficker spread extremely successfully.

 - ▶ [Chapter 4.2](#)

2 Introduction

The ninth semi-annual report (January – June 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 first half of 2009. Chapter 3 covers national topic, 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 Gozi – new Trojan spread via spam e-mails

Already in December 2008, cybercriminals tried to establish themselves in Switzerland with the new Trojan family Gozi, alias Infostealer.Snifula. This was the third e-banking Trojan family targeting clients of Swiss financial institutions.

Using a spam e-mail with suggestive content¹, potential victims were lured onto various prepared pornographic websites. The website then called upon the user to download and install a *Flash plug-in* in order to view the visual content of the Internet page. This download contained the e-banking Trojan.

In January of this year, various spam waves were observed with the goal of spreading the same Trojan type. The spam linked to a bogus page of the free newspaper "20 Minuten". The page was copied 1:1 from the original and could thus only be recognized as bogus by looking at the web address. Excerpts from the "20 Minuten" article were also used in the spam e-mail. That part of the e-mail was therefore also in correct German. The changed and added parts of the e-mail contained mistakes, however. The titles referred for example to the expansion of free movement of persons to Bulgaria and Romania. Since these were specifically Swiss topics, very targeted distribution of the e-mails can be inferred.

From: ZURICH Contact [mailto:alarm@20min.ch]
Subject: ZURICH ALARM: In 2007, only 203 entrants from Eastern European countries were registered.

ZURICH

50% more Eastern European prostitutes

The number of prostitutes from Eastern Europe is growing rapidly: Nearly half of the women newly registered by the Zurich City Police in 2008 were from Eastern Europe.

To detail >>

With the friendly greetings, Roseann Mansfield.

Spam e-mail on free movement of persons

¹ <http://www.melani.admin.ch/dienstleistungen/archiv/01074/index.html?lang=de> (as of: 21.08.2009).



Bogus page of the newspaper "20 Minuten". To watch the video, the user is asked to install a Flash plug-in.

The "20 Minuten" article to which the spam e-mail referred and the text it used was published on Sunday at 10:18 p.m. On Monday morning, the spam e-mails were already sent out. The spam waves were repeated on Tuesday and Wednesday. The content was identical in all waves, but the domains for accessing the pages were different. The pages were hosted on a so-called *fast flux network*, which means that a single page is saved redundantly on several servers². If a server is disabled, the query is automatically redirected to the next server. This makes deactivation more difficult and extends the period of time for successful execution of the attack. The domains were all registered with a registrar in China. This does not indicate the origin of the perpetrators, however.

These were the last major e-mail waves so far to spread e-banking Trojans. Apparently, costs and benefits no longer added up, since too few computers were compromised during spam waves. In total, attacks with e-banking Trojans declined sharply beginning in January. Most attacks switched to other business models such as *rogue software*. *Rogueware* is malware pretending to have found pests on a computer, but only able to remove them with a paid version of the software. *Drive-by infections* are also increasingly used as attack vectors. (See [Chapter 3.2.](#)) More detailed information on fast flux networks is provided in the semi-annual report 2007/2.²

3.2 Drive-by infections on the rise

As already indicated in the last semi-annual reports, a shift of attack vectors (from e-mails with attachments or links) to website infections – so-called drive-by infections – is taking place. The classic ways of spreading malware apparently are no longer working so well, now that users are reacting more sensitively: they no longer click on every link contained in an e-

² <http://www.melani.admin.ch/dokumentation/00123/00124/01048/index.html?lang=en>

Information Assurance – Situation in Switzerland and Internationally

mail or open every strange-looking attachment. According to information by the security firm Scansafe³, 74% of malware in the third quarter of 2008 was already being distributed via websites. The company Websense reports that 70% of the 100 most popular sites contained malicious software at least temporarily or were used by cybercriminals for their activities.^{4 5}

Search engines play a role in drive-by infections that should not be underestimated. Attempts are made to compromise websites that have a high ranking for popular search terms and are also poorly protected or exhibit vulnerabilities. Sometimes, the drive-by infection also contains an evaluation of the *referrer*: in such cases, the drive-by infection is only activated if the site is accessed via a search engine. Since the website administrator generally only accesses the site directly, it may be difficult to detect that the site has been compromised. In the case of a drive-by attack known by the name Gumblar, which was observed in May of this year, the Trojan manipulates the results displayed by the victim's browser in Google searches. The victim is thus induced to access other dangerous sites, which dramatically increases the risk of another infection.

The developments in the field of drive-by infections are remarkable (see Trends, [Chapter 5.4](#)). What is the same in every drive-by attack, however, is the fact that a suitable webserver must first be found via which the infection can be distributed. The attackers therefore hack into existing web servers to place their malicious code there. For this purpose, they use stolen *FTP* passwords or exploit vulnerabilities in the server software. In special danger in such cases are *content management systems (CMSs)* – but also forums, guestbooks, and the associated databases provide a target. Notable in this regard is that when a vulnerability is exploited, not merely a single website is affected, but as a rule other sites as well that are hosted on the same webserver.

The attack itself takes place in several steps. The hacked site contains a *code* that redirects the visitor in the background to a third-party server. In most cases, this happens via *IFrame*, which is often generated using *JavaScript*. In future, automatic redirects, so-called *META refreshes*, should also be expected (see Trends, [Chapter 5.4](#)). The JavaScript concealment is used to make detection of such infections (such as by anti-virus software) more difficult. Meanwhile, *IFrames* are also being placed directly on websites, since this can be even less conspicuous given the widespread sensitivity to JavaScript as an attack vector. As soon as the victim is redirected, several steps are executed to determine what programmes are installed on the computer and whether old versions exist that still contain vulnerabilities. If this is the case, malware tailored to the vulnerability is used to infect the system. Such vulnerabilities not only affect the browser itself, but especially also associated *browser plugins* such as Flash and Acrobat Reader or critical vulnerabilities in the *ActiveX Control* element, etc. If no suitable vulnerability is found, the user is often asked to install the malware manually.

The techniques for placing drive-by infections undetected for as long as possible on a website are improving rapidly. This development is illustrated in [Chapter 5.4](#).

To arm your computer against drive-by infections, please read the chapter on "Countermeasures" in [Annex 7.2](#).

³ http://www.scansafe.com/resources/global_threat_reports2/gtr_2008/Q3_2008_GTR.pdf (as of: 31.08.2009).

⁴ http://securitywatch.eweek.com/exploits_and_attacks/most_popular_sites_were_hacked_in_08.html (as of: 31.08.2009).

⁵ http://securitylabs.websense.com/content/Assets/WSL_ReportQ3Q4FNL.PDF (as of: 31.08.2009).

3.3 Misuse of Swiss e-mail accounts

In the last semi-annual report, MELANI described how access data to Internet services are increasingly being targeted by cybercriminals. The focus then was on the placement of drive-by infections on websites and the misuse of auction accounts. The report also discussed phishing attempts against e-mail service providers such as Bluewin, Hotmail, etc. The last report did not discuss what can be done with a stolen e-mail account. Many users may say that they do not really care if third parties access their e-mails or that the e-mails they receive are not really confidential. But there is more to it than that: Once again, criminals are of course motivated by money. An actual Swiss case shows how money can be made with stolen e-mail login data:

In June 2009, stolen access data was used to log into the e-mail account of a Swiss citizen. An e-mail was sent to all 350 of his contacts, claiming that he was in trouble during a supposed trip to Africa. His passport, all his money, and all other documents had been stolen. To be able to even leave the hotel, he would urgently need 1,000 euros for the hotel bill plus 100 euros for unpaid telephone calls. Of course he would fully reimburse the money as soon as he returned to Switzerland. The money should be sent via Western Union to Abidjan to a person unknown to the e-mail recipient. Because of the circumstances, he could not be reached by telephone.

Fortunately, nothing happened in this case, thanks to the scepticism of the addressees, who absolutely wanted confirmation by telephone from their friend who supposedly was in need, and thanks to their notification of Western Union.

Not only the e-mail 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 their contacts with other persons will be listed in meticulous detail. The goal will be to tailor e-mails to potential victims as closely as possible. Since the effort involved is considerable, this has only been observed so far in the case of sporadic, very targeted attacks. But once these connections are compiled automatically and on a large scale, the effort is reduced considerably, and it must be expected that this technique will be used also for "untargeted" attacks. This will always be done with the intention of inducing the victim to click on an attachment or perform some other action. Caution is therefore called for not only with regard to e-mails from unknown persons, but also from known senders. In the case of unusual occurrences – especially involving money – MELANI recommends verifying information by phone, identifying the person by asking questions only he or she can answer, or discussing the credibility of the story with mutual acquaintances.

3.4 Interrupt of Cablecom Internet and telephone network

A *DDoS attack* against a Cablecom customer caused an interruption on the Cablecom network for more than an hour on 19 January 2009. Internet traffic had increased by several gigabits/second. Internet and telephone services in and around Zurich but also in other regions were limited or no longer available. As a consequence, Cablecom redirected Internet traffic via an alternate Internet connection to the international network. This allowed the attacking traffic to be curtailed at the entry points of the Cablecom *backbone* and the international Internet backbone. Cablecom said that nearly one third of customers in the greater area of Zurich, i.e. about 90,000 subscribers, were affected. It was not possible or difficult for them to make phone calls or use the Internet between 12:50 and 1:50 p.m.

Several DDoS attacks have already been reported in Switzerland. Websites with pornographic content are attacked with particular frequency.⁶ In December 2007, for instance, the website www.sexy-tipp.ch was attacked using a *botnet*.⁷ But also other websites associated with the Zurich brothel scene suffered the same fate. During such attacks, other websites hosted on the same server are often also affected – and in most cases, the entire network is disrupted. Whether this was the cause of the Cablecom attack is unknown. Cablecom filed criminal charges with the police.

3.5 E-mails with malicious software targeted at major companies

In the first half of 2009, a very targeted wave of attacks⁸ was observed against the management of major companies. The e-mails were written in English and claimed that a payment order had been triggered which should be verified by clicking on the attached document named "details.rtf". The malware was then installed upon opening the file.

An example of such an e-mail looks like this:

Subject: Re: Wire Transfer <First and last name of recipient>

The wire transfer has been released.

BENEFICIARY : <First and last name of recipient>
ABA ROUTING# : XXXX92729
ACCOUNT# : XXX-XXX-XXX25
AMMOUNT : \$19,438.16

Please check the wire statement attached and let me know if everything is correct. I am waiting for your reply.
Laura

The analysis of the malware showed that all directories accessed via Windows Explorer, all websites visited with the browser, and all data entered on forms were recorded and sent to various servers. These servers, which were specified permanently in the malware, were able to be identified and deactivated. Similar waves were observed internationally. How many of these e-mails were sent out is unknown, however. The e-mails were practically exclusively aimed at members of company management, which indicates a very targeted attack. Apparently, other spam waves took place at the end of December 2008^{9 10} with the same wording. These had a different attachment, however (bank_statement.scr or bank_statement.zip), and were apparently not sent out in as targeted a manner. It is unknown who is responsible for this wave and what the intention was.

⁶ http://www.pcwelt.de/start/sicherheit/firewall/news/192305/zwei_porno_sites_lassen_streit_escalieren/ (as of: 31.08.2009)

⁷ <http://www.melani.admin.ch/dokumentation/00123/00124/01048/index.html?lang=en> (as of: 31.08.2009)

⁸ <http://isc.sans.org/diary.html?storyid=6511> (as of: 31.08.2009)

⁹ <https://tools.cisco.com/security/center/viewAlert.x?alertId=17321> (as of: 31.08.2009)

¹⁰ <http://fordhamsecureit.blogspot.com/2008/12/wire-transfer-phishing-email-sent-to.html> (as of: 31.08.2009)

4 Current International ICT Infrastructure Situation

4.1 IT espionage against Tibetan NGOs and the office of the Dalai Lama

On the weekend of 29 March 2009, several media reported on a Canadian study on Chinese IT espionage entitled "Tracking GhostNet - Investigating a Cyber Espionage Network".¹¹ The study contained the results of an investigation of IT-based attacks primarily against Tibetan non-governmental organizations and the office of the Dalai Lama, which infected further systems in more than 100 countries. These included systems in companies and government offices.

Already in 2007, confidential reports of the head of the British MI5 were made public¹² which warned of targeted espionage attacks using sophisticated *social engineering methods* and customized Trojan horses. According to the reports, the targets of Chinese attackers included *critical national infrastructures* and government offices. Also in Switzerland, such attacks against government offices have meanwhile taken place. In such cases, the attackers sent prepared documents with bogus senders to key persons in the affected companies. The messages were tailored to the recipients, which indicates that information had been obtained previously by intelligence services.

In light of the available information, it must be assumed that these attacks, referred to as "GhostNet", belong to the same cluster of cases as the attacks against State institutions, critical infrastructures, and companies known and published since a couple of years. The origin of these attacks is suspected to be in China.¹³ Also in Switzerland, infected systems have been found as part of the GhostNet investigations. However, all of these systems have belonged to representations of foreign groups and governments in Switzerland. Swiss companies and government offices have not been part of GhostNet.

4.2 Conficker

The computer *worm* Conficker (also known as Downadup) was one of the main ICT topics in the media in the last half year. Especially around 1 April 2009, the date on which the worm was expected to update itself, media interest was enormous.

The first version of this Windows worm had been circulating already since 21 November 2008. This changed dramatically at the beginning of the year, however. To spread, the worm uses a vulnerability in the Microsoft Windows Server Service (MS08-067), which, however, already received a security update at the end of October 2008. The threat was therefore primarily effective against companies and individuals who had not installed this update. The worm has another option to spread, however: It goes through a list of simple passwords¹⁴ to copy itself to network permissions, or it tries to copy itself to mobile data carriers such as *USB sticks* and digital cameras. As soon as an infected USB stick is plugged into a

¹¹ <http://www.news.utoronto.ca/media-releases/international-affairs/information-warfare-monitor.html> (as of: 31.08.2009)

¹² <http://www.melani.admin.ch/dokumentation/00123/00124/01048/index.html> (as of: 31.08.2009)

¹³ <http://www.melani.admin.ch/dokumentation/00123/00124/00161/index.html> (as of: 31.08.2009)

¹⁴ http://blog.namics.com/2009/02/die_aktuelle_li.html (as of: 31.08.2009)

Information Assurance – Situation in Switzerland and Internationally

computer, it opens a window in which the worm creates a standard icon for opening directories. The icon is not located in the Options area, however, but rather in Start Program. Clicking on the icon installs the worm on the computer. Conficker is estimated to have infected several million computers.

Once the worm is installed, it stops the Windows Update processes and creates a local webserver. It then tries to spread further and disguise itself, in order to make it more difficult to remove. It can download and execute files as desired. Finally, it blocks access to many security sites and anti-virus update services.

The update mechanism and the magical date (1 April 2009) in particular on which the worm was expected to update itself generated huge media interest. The update mechanism uses an algorithm to generate domain names with which it tries to enter into contact to download an update. Conficker.C was in theory able to generate 50,000 domain names a day with which it could have entered into contact. If the contact attempt fails, the worm waits 24 hours and generates 50,000 new domain names. As was the case with previous worms, the authors' primary goal in the first few months was to install and protect the botnet (consolidation of the network), rather than use the botnet for any spectacular actions. This is also indicated by the fact that the programmers of the worm used the most modern algorithms, some of which were only just a few weeks old. The built-in encryption technique used to protect from misuse by other hackers was only developed in autumn 2008. It could therefore be expected that the Internet would not be hit by major interference on 1 April. Only on 7 April 2009 did the security firm Trend Micro observe enhanced *P2P activity* by Conficker.C, which converted the worm into the Conficker.E variant. Again, the main motivation of the worm was to cover its tracks. It blocked sites offering worm removal programmes. It also appeared under a random file name and deleted all its tracks on the host computer. One can only speculate about the exact motivation of the Conficker developers. One motive might be to establish a *botnet* for renting out to other criminals. It is known that Conficker.C installs the *scareware* programme SpywareProtect2009.¹⁵

Numerous corporate and government networks abroad were hit by this worm, for instance the hospital and provincial government of Carinthia¹⁶ and the German Federal Armed Forces¹⁷. Also in Switzerland, corporate networks were disabled by the worm for several hours. Infected computers were found behind about 1,000 *IP addresses* in Switzerland. Most infected computers were located in Russia, Brazil, China, and India, however.

Problem of certified systems

It was particularly striking that the worm mainly affected networks in the healthcare sector¹⁸. The reason was likely that these networks have an especially high number of certified computer systems (such as steering systems for examination devices), which cannot simply be patched. If such systems are also connected to the Internet, they are an easy target for the worm. Another problem is the use of personal laptops and USB devices in company networks. This may allow infections to move from private computers to the company network. The worm perfectly exploits this weakness.

¹⁵ <http://www.heise.de/security/Deckt-der-Conficker-Wurm-jetzt-seine-Karten-auf--/news/meldung/136083> (as of: 31.08.2009)

¹⁶ <http://www.heise.de/security/Conficker-in-Kaernten-Nach-der-Landesregierung-nun-die-Spitaeler--/news/meldung/121570> (as of: 31.08.2009)

¹⁷ <http://www.netzwelt.de/news/79475-conficker-bundeswehr-kaempft-gegen-computerwurm.html> (as of: 31.08.2009)

¹⁸ <http://diepresse.com/home/techscience/internet/sicherheit/473436/index.do> (as of: 31.08.2009)

No one actually had still been expecting such a worm outbreak. After the introduction of WindowsXP with Service Pack 2, which contains a firewall and regularly downloads the newest updates, everyone should actually be protected from this kind of worm. The reality is different, however. One thesis is that most of the compromised computers were not running official Windows versions, so that users deliberately did not take advantage of contacting the Windows Update servers.

Once again, it was shown how important the basic protection of a computer is. This includes updating the operating system and applications, a firewall, and updated anti-virus software. Since updates are not immediately updated in many companies and must first be tested for compatibility with other programmes, a delay may occur in installation, which should be kept as brief as possible, however. With the widespread use of USB sticks, digital cameras, mobile phones, and *MP3 players*, infection routes via mobile storage media will become increasingly prominent.

4.3 SCADA

Supervision, control, and data acquisition for industrial facilities, utilities for distributing vital goods (electricity, water, fuel, etc.), and transport and traffic systems (railways, traffic management systems, postal services, etc.) have long been unthinkable without information and communication technology (ICT). The development and operation of such *supervisory control and data acquisition* (SCADA) systems has a long tradition. Originally, SCADA systems had little similarity with traditional ICT: they were isolated from computer networks, used proprietary hardware and software, and used their own protocols for communicating with the central computer. The widespread availability of comparatively inexpensive devices with built-in interfaces to the *Internet Protocol* (IP) has resulted in major changes in this area in recent years. Sensors, machines, and switches now more and more frequently have their own IP address and use the normal Internet Protocol for communicating with the central computer. The advantage of using conventional low-cost ICT is purchased by the fact that SCADA systems are now in principle exposed to the same threats that we know from the Internet; they are now open to malware and hackers. The debate on the security of SCADA systems is thus becoming increasingly widespread, as shown by the examples below. The attacks on these systems, which are key to the smooth functioning of our society, are not just hacker attacks (sabotage), but also technical failures that can lead to the breakdown of important systems, as the example of the *ETCS* system interrupt of the Swiss Federal Railways (SBB) in summer 2009 shows.

ETCS interrupt causes a detraction of the railway traffic between Mattstetten and Rothrist and in the Lötschberg tunnel

The abbreviation ETCS¹⁹ stands for European Train Control System, a pan-European harmonized SCADA system for train protection. The standardization applies especially to the transmission of information between the track system and the vehicle. The information transmitted via ETCS components is usually gathered or generated using the existing safety installations.

On the new tracks between Mattstetten and Rothrist, in the Lötschberg tunnel, and in the Gotthard base tunnel still under construction, ETCS Level 2 is used. At speeds greater than 160 km/h, the engine driver is no longer able to recognize the signals visually. Moving

¹⁹ <http://mct.sbb.ch/mct/etcs-technologie-funktionsprinzip.htm> (as of: 31.08.2009)

Information Assurance – Situation in Switzerland and Internationally

authority and other signal aspects are therefore displayed in the driver's cab. However, the track-release signalling and hence the train integrity supervision still remain in place at the trackside. All trains automatically report their exact position and direction of travel to the control centre at regular intervals. Train movements are monitored continually by the control centre. The movement authority is transmitted to the vehicle continuously via *GSM-R* together with speed information and route data. This system failed on 29 July 2009, which had major impacts on the entire SBB route system. While conventional signals still exist on the Mattstetten-Rothrist route, allowing trains to drive at speeds up to 160 km/h, no signals are available in the Lötschberg tunnel, which led to a rerouting over the old Lötschberg route.

Attackers allegedly penetrated control system of the US electricity grid

Attackers apparently succeeded in installing software in control systems able to disrupt important systems such as the electricity and water supply of the United States. A vulnerability is said to have been exploited. According to a report in the Wall Street Journal²⁰ citing US security authorities, attackers penetrated the US electricity grid and deposited programmes in the system that could be used to disrupt the electricity supply in the entire country. According to the report, the US authorities believe that the attackers' goal is to steer the US electricity grid. So far, they have not tried to damage the infrastructure, a fact that could change rapidly in the event of a crisis or war, however.

Planned *smart grid* vulnerable to attacks

Smart grids are envisaged as a replacement for conventional grids. The Californian company Pacific Gas and Electric, for instance, wants to distribute intelligent gas and electricity meters to their clients by 2011. Intelligent electricity meters would be installed with end users, directly reporting collected data on the electricity or gas consumption of customers to the utility's grid nodes. Given the higher density of data, this would also allow better distribution and adjustment. Partial grid power cuts could also be detected more rapidly. According to a sealed study, these devices appear to have several security weaknesses, however. The employed protocols also do not contain security measures. If these weaknesses were to be exploited by a potential attacker, this might lead to an electricity power cut. For instance, an attacker could signal high demand. If the electricity producer reacts to this supposedly high demand, it may lead to an electrical surge in the grid. The transmission path used is the *frequency-hopping spread spectrum (FHSS)* between 902 and 928 MHz, but also *WLAN* and *GPRS* technologies. Currently, intelligent electricity meters are only being used in pilot projects. This will likely change in the near future, however. The US and also Europe will start using more smart grids from 2011.

British experts warn against use of Chinese telecommunication components

According to statements by British experts,²¹ components of the Chinese telecommunication company Huawei may be used to trigger disruptions of important infrastructures in the United Kingdom such as telecommunication, electricity, and water supply. Key components of the new communication network of British Telecom are supplied by Huawei. Huawei is one of the largest telecommunication suppliers worldwide with more than 87,000 employees. It is a private company not listed on the stock market. The focus of its products is the development and manufacture of communication technology devices, especially in the fields of mobile communications, xDSL, optical networks, and end devices. The doubts of the British experts could, however not be verified or proven in any case.

²⁰ <http://online.wsj.com/article/SB123914805204099085.html> (as of: 31.08.2009)

²¹ <http://www.telegraph.co.uk/news/worldnews/asia/china/5072204/Britain-could-be-shut-down-by-hackers-from-China-intelligence-experts-warn.html> (as of: 31.08.2009)

While the control of infrastructures used to be low-tech and thus more or less easily comprehensible, the functions of hi-tech devices can no longer be verified so easily. More and more, the selection of devices and the award of project contracts for (critical) infrastructures should therefore no longer pay attention only to the purchase price, but also to the (long-term) security offered. It should also be carefully considered whether SCADA systems should be operated only with logical separation from other enterprise networks or also with physical separation. The use of redundant systems is also recommended, in order to maintain operations of the infrastructure even in the event of breakdowns or damage. The failure of telecommunication (especially Internet connections), electricity, and transport systems may entail enormous costs for both companies and individuals.

4.4 Increased focus on military units for information warfare in various countries

Information warfare is far up on the list of government offices around the world responsible for defence and warfare – not only since the massive *denial-of-service* attacks on Estonian government and corporate networks in 2007. In Germany, for instance, a Federal Armed Forces body of troops has been constituted to deal with *network-centric operations (NCO)*.

In line with general technological convergence and networking (see [Chapter 5.1](#)), military guidance, communication, and control systems are increasingly part of integrated networks and thus potential targets by means of information and communication technology. This entails that in the case of military conflict, not only the use of conventional military means may be considered, but also direct attacks on the enemy's networks. Conversely, every military force must now be concerned with absolute protection of their increasingly networked systems.

It is well known that the large military powers in particular such as the United States and China have undertaken major efforts in this regard in recent years. The development of capacities is likely not restricted to defensive, network-protecting means.

Also in Switzerland, the concept of "information operations" has been evaluated more carefully since 2001. A concept study on this topic has been prepared, the initial conclusions of which have resulted in establishment of a *CERT* for military installations called "MilCERT".

Certain fundamental political and legal questions must be raised regarding such initiatives, however. In principle, it is clear that the military units of a State must have possibilities at their disposal to protect their systems against ICT-aided attacks by the enemy. This may in certain circumstances entail, however, that offensive means are used to disable or disrupt the opponent's systems before an attack on one's own networks can be carried out. These means may also be used as additional means of warfare during armed conflict. But especially in an era when classical armed disputes between States are the exception, and conflicts are generally carried out below the threshold of war, the offensive use of military ICT means is very tempting, although it leads one onto shaky international legal ground.

In the case of the attacks against Georgian government systems, the term "cyberwar" was used strikingly often. However, these attacks against the State computer systems and networks were primarily of a purely criminal nature. The attacks, while carried out during an armed conflict, were thus of a civilian nature and would therefore have to be properly classified as an illegal offence and prosecuted as a crime in the State of the injured party.

Information Assurance – Situation in Switzerland and Internationally

The operation of a group of activists in Israel during the Gaza War²² should also be understood in these terms. One could argue, however, that both cases could nevertheless fall under the law of war, since they were operations carried out in the context of an armed conflict between two States or State-like parties.

Sudden blurring of these boundaries and classification of such collateral actions as acts of war, with consequent reciprocation by means of military ICT operations, would at the same time represent an expansion of the legitimization of military measures against non-military parties participating only indirectly in the armed conflict.

When developing and employing offensive civil or military ICT capacities, it must be determined precisely for what purpose, in what cases, and especially against whom and under what circumstances these capacities may be used. Not every attack against military or State networks as such is an act of war – even if the State may actually be engaged in armed conflict. There are also problems with a clear attribution if it comes to such attacks. A clear author, usually cannot be found and counter-attacks might lead to unforeseeable collateral damages within the target country. The examples in Estonia and Georgia show that such attacks may very well be solely of a criminal nature and accordingly should be prosecuted as criminal offences. Blurring this clear dividing line harbours the danger of employing existing means unnecessarily to interfere with core areas of civilian institutions primarily responsible for protecting internal security. This also would entail that the rules of proper law enforcement and especially the protection of the fundamental rights of the accused would be violated even when no emergency situation exists.

4.5 More politically motivated DDoS attacks

According to the security firm Arbor Networks²³, politically motivated Internet attacks are becoming increasingly widespread. Both the frequency of attacks and the number of targets is rising steadily. A possible reason could be that even technically untrained people can purchase and use DDoS tools such as "Black Energy" or "NetBotAttackers". These tools can be operated using a simple interface. This was also shown in a BBC experiment (see [Chapter 4.7](#)). Although until recently DDoS attacks against porn websites predominated, it has become clear at the latest since the attack against Estonia that this technology can also be used as a political weapon. In addition to attacks in Georgia²⁴, Russian hackers in January 2009 managed to cut off Kyrgyzstan²⁵ from the Internet. The attack was aimed at the two largest Internet providers. One can only speculate what the attackers' motives were, but they likely also had a political background.

A steady increase in quality has been observed in the field of DDoS attacks. The number of computers needed to carry out an attack is becoming smaller and smaller. Using so-called DNS amplification attacks, for instance, a small botnet can have a major impact. In one case²⁶, data transfer of 5 gigabytes/second could be achieved using only 2,000 computers.

²² <http://www.heise.de/newsticker/Gaza-Konflikt-Der-Krieg-im-Internet-/meldung/121389> (as of: 31.08.2009)

²³ <http://www.arbornetworks.com> (as of: 31.08.2009)

²⁴ <http://www.melani.admin.ch/dokumentation/00123/00124/01065/index.html?lang=en> (as of: 31.08.2009)

²⁵ http://www.pcwelt.de/start/sicherheit/firewall/news/192009/russische_cyber_miliz_attackiert_kirgisistan/ (as of: 31.08.2009)

²⁶ http://www.pcwelt.de/start/sicherheit/firewall/news/192305/zwei_porno_sites_lassen_streit_escalieren/ (as of: 31.08.2009)

4.6 T-Mobile network failure

Beginning at about 4 p.m. on Tuesday, 21 April 2009, no communications were possible on the mobile network of T-Mobile in Germany. This was the largest failure so far of a mobile communications network in Germany²⁷. All voice and SMS services broke down. The reason for this failure was a software error in the *Home Location Register (HLR)* which is responsible for establishing the connection between the mobile station and the associated mobile network number. A failure in the HLR means that no connections can be established and the network is no longer reachable. Once the failure was fixed, the network became partially available again at 7 p.m.

On 25 June 2009, the telephone network of E-Plus was also disrupted throughout Germany for about two hours. In this case, the source was reported to be an error in the central proxy server²⁸.

In both cases, a central component appears to have been responsible for the failure. These systems are in general set up redundantly in order to prevent such a breakdown. This is very good protection against hardware failures, i.e. the breakdown of a server. At least in the case of T-Mobile, however, the problem appears to have been a software error. Since roughly the same software and configuration runs on redundant systems, it is not astonishing that the same software problems arose on the backup system as on the main system, causing the backup system to crash as well.

It should be emphasized that in the case of T-Mobile, there were difficulties mobilizing the repair service. Since the responsible technicians are generally called up using the company's own mobile network, they were difficult to reach. With the spread of mobile telephones, the availability of repair and also emergency services will increasingly rely on the mobile network. The consequences that the failure of this network can have on emergency services must always be taken into account.

4.7 UK: BBC acquires botnet for demonstration purposes

In preparation for a programme on Internet crime, the British broadcaster BBC acquired the control software for a *botnet*. According to the BBC, the network (called "Click" after the BBC programme of the same name) consisted of about 22,000 *zombie computers* at the time of the acquisition. The BBC found the botnet software by visiting chatrooms. In such chatrooms, criminals enter into contact with each other and offer their services. A botnet is a collection of computers infected with malware that can be controlled remotely by an attacker. The BBC apparently paid about 700 dollars for the 22,000 bots. This was relatively inexpensive, since the botnet was non-specific and distributed around the world. The better the quality of the botnet, the more expensively it can be sold. BBC mentioned prices of between 300 and 400 dollars per 1,000 bots. For demonstration purposes, two test e-mail addresses were flooded with thousands of spam messages over the course of a few hours. According to the BBC, one website was disabled using a distributed denial-of-service (DDoS) attack in consultation with the provider. It turned out that network requests by only 60 computers would already have sufficed to disable the website. The affected computer users have meanwhile been

²⁷ <http://www.welt.de/webwelt/article3603796/T-Mobile-schenkt-Gratis-SMS-als-Entschuldigung.html> (as of: 31.08.2009)

²⁸ http://www.zdnet.de/news/wirtschaft_telekommunikation_e_plus_netz_gestern_90_minuten_lang ausgefallen_s tory-39001023-41005882-1.htm (as of: 31.08.2009)

Information Assurance – Situation in Switzerland and Internationally

informed of the occurrences. For this purpose, a warning message was displayed on the desktop of the infected systems.

This approach raises the question of whether, for instance, a security firm could take over and manipulate a botnet to uninstall it or display a warning message on infected computers like in the BBC case. Whether this is a way to combat botnets will certainly be discussed more intensively in future. The acquisition of botnets would likely be counterproductive, however, since it would further encourage the market for botnets and make it more lucrative for cybercriminals to set up a botnet. The BBC report showed very clearly, however, that a botnet can be controlled with simple programmes that can also be operated by people who are not computer specialists. The trend in this field goes even further, however. Last year, cybercriminals developed the model of crimeware-as-a-service²⁹. Cybercriminals aware of the technical possibilities can use this model to "rent" such a service. They can receive the service directly via these platforms and do not have to deal with technical problems. It can be expected that this new model will experience a development surge in 2009.

4.8 US: Massive increase of data mishaps in 2008

According to San Diego-based Identity Theft Resource Center³⁰, a total of 35 million datasets were lost in the US in 2008. Compared with the previous year, this represents an increase of 47% of data losses reported by companies and authorities. Most data leakages occurred in the private sector. According to the study, the financial sector and credit card companies are taking the most countermeasures. The Identity Theft Resource Center lists five categories responsible for the data losses: loss of digital data carriers (laptops, USB sticks, etc.), internal and external data theft, unintended publication and dissemination of personal information, and loss of data by external service providers.

It can be expected that more and more data will be stolen and lost, but also that pressure will increase to report data mishaps. In Switzerland, no official information is available on the number of such mishaps. The national data protection legislation does not contain any explicit norms requiring owners of data collections to report data mishaps. But also in Switzerland, incidents have become known such as the publication of confidential data on the Schengen agreement on the website of the Federal Department of Justice and Police (FDJP) in May of last year.³¹

With a view to the many ways in which data can be lost, it is apparent that an integral security concept must focus on protection of the information itself. Distribution channels, access rights, and storage locations must be adjusted to the actual value of the information. Not every channel or storage location is equally safe, and not all documents are equally sensitive. This necessitates better risk management in dealing with data and information. Sensitization of employees is of the utmost importance. Technical protection measures are part of basic data protection, but they may be ineffective when information is handled carelessly. In most cases, the weakest and most vulnerable link in the security chain continues to be the human being.

²⁹ SAR 2008/II point 5.2 <http://www.melani.admin.ch/dokumentation/00123/00124/01085/index.html?lang=en> (as of: 31.08.2009)

³⁰ <http://www.idtheftcenter.org/> (as of: 31.08.2009)

³¹ <http://www.melani.admin.ch/dokumentation/00123/00124/01065/index.html?lang=en> (as of: 31.08.2009)

4.9 US wants to strengthen measures against cyber threats and improve protection

At the beginning of the year, the new US government under Barack Obama published its agenda on the security of the United States. The country's electronic networks are declared to be a "strategic good", and great importance is attached to the protection of the national IT infrastructure. To coordinate the various agencies dealing with this topic, a "National Cyber Advisor", also called "Cyber Czar", reporting directly to the president will be appointed. A "Safe Computing Research and Development Effort" was also announced for purposes of developing a new generation of especially secure hardware and software for official networks.

At the end of May, the "Cyberspace Policy Review" was published, a status report on the current situation in cyberspace, with recommendations for further steps to be taken by the United States in this field. The authors concluded that the Internet will fuse with traditional telecommunication technologies over time, and that other infrastructure operators will increasingly use this network as the primary channel for the interconnectivity of systems (see also SCADA, [Chapters 4.3](#) and [5.2](#)).

Operation of the Internet, like many other infrastructures for basic physical utilities, is generally ensured by private actors. The Cyberspace Policy Review also recognized that cooperation with these private actors is indispensable for security in this field. The State as well as private operators of important infrastructures have a fundamental interest in the reliable functioning of the technologies employed and secure data transmission within the information infrastructures. For this reason, a "public-private partnership for cybersecurity" is also being recommended in the United States to encourage participants to jointly ensure better protection as well as more security and robustness of the digital environment by way of information exchange and coordinated activities. It has also been recognized that problems relating to the Internet cannot be solved by the United States on its own, but rather must be addressed in an international context. One goal must therefore be to improve the preconditions for a secure and strong digital nation at home by revising the relevant legal foundations and guidelines, and to create a framework for coordinated measures by the involved actors at all levels (local, national, international) when incidents in cyberspace occur.

4.10 EU Commission wants to improve protection of critical infrastructures

The EU has likewise recognized that ICT is increasingly becoming entwined with the everyday life of their citizens and represents an indispensable part of economy and society, since it either provides goods and services of fundamental importance or constitutes the basis for other critical infrastructures.

Due to the ever greater dependence on critical information infrastructures, their cross-border networking and linkages with other infrastructures, as well as their vulnerability and threats, it is crucially important to systematically improve the security and robustness of these infrastructures. In this way, they must be in the front line to defend against outages and attacks, since disruptions of critical information infrastructures may seriously interfere with important social functions.

Information Assurance – Situation in Switzerland and Internationally

The most recent attacks on information infrastructures in Estonia, Lithuania, and Georgia have shown that important electronic communication services and networks are constantly under threat.

In its Communication of 30 March 2009 on Critical Information Infrastructure Protection³², the EU Commission therefore calls for measures to enhance the security, robustness, and resilience of the Internet and of critical information infrastructures in general. To achieve this, the Commission wants to promote public-private partnerships. The Commission is also planning joint capacities and services for pan-European cooperation, a forum for information exchange among member States, and a European information and early warning system. It calls upon the member States to prepare national emergency plans and to regularly conduct emergency exercises to test the response to major network security breaches. Cooperation of the national CERTs and CSIRTs will naturally also be strengthened further.

The EU is consequently paying greater attention to protection from major cyber attacks and disruptions by strengthening its preparedness, security, and resilience.

4.11 Facebook changes its terms of service – for a short time

Facebook revised its terms of service the beginning of February. Already before, Facebook had an irrevocable right to use all published data. The changes to the terms of service were intended to extend this right of use to deleted data as well. After massive protests, Facebook decided to return to the old terms of service.³³

³² <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF> (as of: 31.08.2009)

³³ <http://www.heise.de/newsticker/Facebook-nach-dem-AGB-Debakeel-/meldung/133094> (as of: 31.08.2009)

5 Trends / Outlook

5.1 Cloud computing, outsourcing, centralization, and information ownership

On 17 May 2009, Swiss voters approved the introduction of *biometric passports* by a bare majority of 50.1%. Along with concerns relating to data protection, an argument arising from the field of information assurance appeared to be partially responsible for the tight outcome. This concerned the way in which biometric data was to be stored, namely centrally by the Federal Office of Police (fedpol) on behalf of all cantons. During the voting campaign, this solution was repeatedly called a risk concentration. If the data were to be stored in each home canton, a single successful attack would not affect all datasets, but only a part thereof. To obtain all biometric records, 26 successful attacks on cantonal data centres would be necessary in the best case, not just one attack at the federal level.

Especially in the field of information assurance, such risk considerations are a daily occurrence. While ICT security is still one of the main pillars of a functioning information assurance concept, the focus is increasingly on the protection of information itself. This involves a classical risk assessment and management process. For instance, the blocking of Facebook in companies is not only due to considerations of productivity, but also is certainly due to security-technological reasons. However, one of the greatest risks of *social networking sites* is that individuals can be linked to their employer, which may be in certain circumstances be undesirable in sensitive areas. In such cases, only clear rules governing the proper way to handle information help, whether in private or at work and irrespective of the technology used. It must be clearly defined whether and how data can be disseminated or should be protected.

This development toward strict information ownership and continuous classification of the value of individual information, data, and documents is impeded by the tempting and cost-efficient possibilities of centrally administered and maintained databases, applications, and platforms – in particular developments such as cloud computing, de facto *social networking* monopolies such as Facebook, but also SCADA systems aiming to achieve centralization, real-time reporting for executives³⁴, and efficiency. *Cloud computing*, for instance, promises integrated applications, document preparation, and document management, provided by a trustworthy third-party supplier that is also responsible for the security of the overall system. Different patch levels, applications, etc., within the same company thus belong to the past. However, this also leads to a concentration of risk and, in certain circumstances, a single point of failure. Determining priorities in information management, efficiency and costs, but also the self-administration of systems (security and maintenance) is ultimately the responsibility of each company.

It can be expected that in future the tension will increase between cost pressure, efficiency, and availability of information on the one side, and risk concentration, business outsourcing of critical information and data, and increasing vulnerabilities due to uniform, networked platforms on the other side. The solution to this conflict of objectives and interests must be the result of a case-by-case risk assessment that is as fully informed as possible. The main focus must be on the value of the information belonging to the business that must be protected.

³⁴ <http://www.melani.admin.ch/dokumentation/00123/00124/01048/index.html?lang=en> (as of: 31.08.2009)

The distrust expressed with regard to the centralized storage of biometric data at the federal level is a promising sign in this regard. However, this distrust should also apply to private solutions of a similar type, such as the numerous client profiles that many companies compile and maintain.

5.2 SCADA

The transformations in the field of SCADA systems will continue to advance, and economic pressure will entail that not only individual components, but increasingly also entire substations will be remote-controlled and operated without staff. Moreover, the same network technology throughout the entire system simplifies the desire of management to connect the business network with the control network. The intelligent electricity meters to be employed in the newly planned US electricity grid are one example of this. This development will in future confront ICT security with additional challenges. The goal will be to prevent that incidents such as the importation of malware into the company network spread to the control network. This will make it indispensable to apply principles of traditional ICT security or equivalent standards and guidelines to control systems as well and to demand sufficient security mechanisms from the manufacturers of the devices employed. A comprehensive package of measures also includes exchange of experience among operators of control systems (such as regarding vulnerabilities) as well as between operators and authorities, who in turn can contribute information on current threat situations. The Reporting and Analysis Centre for Information Assurance, MELANI, is in close contact with Swiss electricity utilities and participates in the international exchange of information.

5.3 General cybercrime developments

MELANI and CYCO³⁵ still receive daily reports on a wide range of incidents relating to advance payment scams, supposed lottery winnings, and free offers. Apparently, this kind of Internet crime is still successful. This is also seen in reports from countries from where such scams are committed. Some perpetrators in those countries have been able to fraudulently obtain substantial sums of money in a very short time. The profits allegedly made with so-called subscription traps every day are also drawing attention. In addition to all the technological developments relating to the dissemination and use of Internet malware, the possibility is also available to obtain large sums of money without significant technical know-how, but rather with the requisite persistence, endurance, and creativity. In the huge pool of Internet users, an attacker with sufficient patience can almost always find a victim. Other information on types of fraud and relevant warnings can be found here^{36 37}.

Example: Advance payment scam, lottery scam

This type of scam involves mass sending of e-mail messages to potential victims. The offers and promises made in these messages are entirely made up and are intended merely to create a credible backdrop against which the scam can be perpetrated. E-mails concerning supposed lottery winnings also continue to circulate. They are also a subtype of advance payment fraud.

³⁵ CYCO: Cybercrime Coordination Unit (<http://www.kobik.ch>)

³⁶ <http://www.den-trick-kenne-ich.ch/4/de/> (as of: 31.08.2009)

³⁷ <http://www.fedpol.admin.ch/fedpol/de/home/aktuell/warnungen.html> (as of: 31.08.2009)

Information Assurance – Situation in Switzerland and Internationally

This scam works, as reports from Ghana show. The phenomenon of "Sakawa" occurs there^{38 39}. The perpetrators are generally young men from lower income strata who are trying to get rich quick. The criminal activities, which are usually run out of Internet cafés, meanwhile include almost everything known from other countries in the region as well, especially Nigeria. The rapid spread of Sakawa can be explained by the fact that many perpetrators have succeeded in fraudulently obtaining substantial sums of money in a very short time and that they flaunt their wealth for everyone to see – which in turn of course motivates many others to do the same. Arising in the context of cybercrime, Sakawa has meanwhile also spread to common, locally perpetrated crimes (including killings⁴⁰), the goal of which is to make money.

Example: Free offers

MELANI is receiving a growing number of reports of persons who, after registering on a website, receive a subscription invoice followed by overdue notices. These offers try to get Internet users to conclude contracts or purchase services rapidly, without providing clear information on costs and other terms of service. Once such a "contract" has been concluded, overdue notices and collection orders are sent to intimidate clients. Sometimes, the letters are sent by lawyers or collection agencies to make victims nervous and get them to pay the questionable demands "voluntarily". These sites are generally set up in German. The providers are becoming more and more creative and brazen. Invoices and overdue notices are also often sent out to individuals who never registered on such a site.

Until now, the goal has primarily been to lure Internet users to such sites via search engines. Various offers of this sort appear at the top of Google search results for specific key words. Apparently, attempts are now made to reach users by e-mail⁴¹. The techniques are constantly improving to hide costs from users as effectively as possible. While costs used to be hidden with very small fonts or in the terms of service, animated images are now being used. The price is then only displayed after a few seconds, so that the victim hardly has the chance to recognize it. Here again, business is booming. Between 15,000 and 20,000 euros are paid into the suppliers' accounts every day⁴².

The State Secretariat for Economic Affairs (SECO) recommends not paying this type of invoice and, as soon as the error is discovered, immediately explaining to the supplier by registered mail that the website in question is deceptive and the contract is therefore being contested. SECO further says that a single letter is sufficient; subsequent correspondence from the supplier can be ignored.

For more information in this regard, please consult the following brochure:

<http://www.news-service.admin.ch/NSBSubscriber/message/attachments/7979.pdf> .

³⁸ <http://www.ghanaweb.com/GhanaHomePage/features/artikel.php?ID=162565> (as of: 31.08.2009)

³⁹ <http://www.modernghana.com/news/192603/1/female-sakawa-hits-accra.html> (as of: 31.08.2009)

⁴⁰ <http://www.GhanaVoices.wordpress.com/2009/08/13/girls-killed-for-sakawa/> (as of: 31.08.2009)

⁴¹ <http://www.melani.admin.ch/dienstleistungen/archiv/01089/index.html?lang=en> (as of: 31.08.2009)

⁴² <http://www.pressebox.de/pressemeldungen/ct/boxid-261364.html> (as of: 31.08.2009)

5.4 Drive-by infections

Drive-by infections will increasingly improve in future so that it will be more difficult to detect them. Today, drive-by infections are in most cases uploaded to the website statically. For this purpose, the attacker uses a list of FTP login data, for instance. The data is used to log into the account automatically, then a webpage is downloaded (usually the *index page* or into an existing JavaScript file .js), the malicious code is smuggled in, and the page is uploaded again. The user can naturally also obtain access by exploiting a *vulnerability*. However, the uploaded script is visible to every user, including the web administrator, and is thus detectable.

Already last year, techniques existed to make detection more difficult, especially by web administrators. In June 2008, a large number of Swiss websites were hacked and supplemented with a malicious JavaScript. The perfidious aspect of this attack was that a normal visit to the page would not trigger execution of the malicious code. If, however, the page was accessed via a search engine like Google or Yahoo, the malicious code was activated. The reason for this concealment tactic is that the website owner often accesses his own site, but does this generally directly or via a bookmark. This tactic contributes to keeping the infection hidden for as long as possible.

While the abovementioned example was still accomplished using a static JavaScript and could be detected by analyzing the source code, new trends already signal a further development. The code is then no longer placed directly on the website, but rather brought in via the webserver. Every time the site is visited, a decision is made whether or not to include the code, and if so, on which page. This makes it practically impossible for the webmaster to reproduce the infection. In a current case that also affected a Swiss *hosting provider*, the attack also appears to run via a compromised FTP account. A *PHP script* was then uploaded to the server. Not the website, but rather the webserver was then manipulated in such a way that it from time to time redirected the visitor to a specific page containing malicious code. A *cookie* that installs the malware helps the attacker to identify the computer. The redirects are then no longer hidden just behind the index pages, but also behind images and *favicons*.

Rather than in IFrames, the redirects are hidden in the META refresh command. In browsers, these redirects are turned off even less than the IFrame command. In combination with a one-time display of the code, this makes it almost as difficult to detect as an IFrame exploit.

To arm your computer against drive-by infections, please read the chapter on "Countermeasures" in [Annex 7.2](#).

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>.

ActiveX	Una tecnologia sviluppata da Microsoft, che consente di caricare piccoli programmi – i cosiddetti ActiveX Controls – sul computer del visitatore al momento della visualizzazione di pagine Web, dove vengono poi eseguiti. Essi permettono di convertire diversi effetti e funzioni. Purtroppo questa tecnologia viene sovente sfruttata in modo abusivo e rappresenta pertanto un rischio per la sicurezza. A titolo d'esempio, sul computer vengono scaricati ed eseguiti Dialer. I problemi di Active-X concernono unicamente
---------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Information Assurance – Situation in Switzerland and Internationally

	Internet Explorer dato che gli altri browser non supportano questa tecnologia.
Biometric passport	Passport with electronically readable biometric data. Personal data such as name, sex, date of birth, etc., are recorded on an RFID chip.
Botnet	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.
Bot / Malicious Bot	Comes from the Slavic word “robota” meaning work. Refers to a program that automatically carries out certain actions upon receiving the command. So-called malicious bots can control compromised systems remotely and have them carry out arbitrary actions.
Browser plug-in	Software, which provides web browsers with additional functions, e.g. so as to show multimedia content.
Buffer overflows	Buffer overflows are one of the most frequent vulnerabilities in current software. They can also be exploited via the Internet. Buffer overflows occur because of errors in the programme that write excessively large data volumes into a reserve memory area, the buffer, that is too small. This overwrites information located after the target memory.
Computer Emergency Response Team (CERT)	Computer Emergency Response Team CERT (also CSIRT for Computer Security Incident Response Team) refers to a team that coordinates and takes measures relating to incidents in IT significant to safety.
Cloud computing	Cloud computing (synonym: cloud IT) is a term used in information technology (IT). The IT landscape is no longer operated/provided by the provider himself, but rather obtained via one or more providers. The applications and data are no longer located on a local computer or corporate computing centres, but rather in a cloud. These remote systems are accessed via a network.
Code	Programme instructions that tell the computer what commands to carry out.
Content management system (CMS)	A content management system (CMS) is a system that makes possible and organizes the joint preparation and processing of content, consisting of text and multimedia documents, generally for the World Wide Web. An author may operate such a system even without programming or HTML knowledge. The information to be displayed is referred to as "content".
Cookie	Small text files stored by a web page when viewed on the user's computer. For example, with the assistance of cookies, user preferences for a web site may be stored. However, cookies can also be abused to compile an extended user profile about one's surfing habits.

Information Assurance – Situation in Switzerland and Internationally

Domain Name System	With the help of DNS the internet and its services can be utilised in a user-friendly way, because users can utilise names instead of IP addresses (e.g. www.melani.admin.ch).
DoS attacks	Denial of service attacks. Have the goal of causing a loss of a specific service to users or at least to considerably restrict the accessibility of the service.
Drive by infection	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.
European Train Control System (ETCS)	The European Train Control System (ETCS) is a component of the uniform European railway guidance system. ETCS is intended to replace the multiplicity of train protection systems employed in different European countries. It will be used for high-speed trains in the medium term and later throughout the entire European railway system.
Fast flux	Fast flux is a DNS technique used by botnets to conceal phishing or malware-spreading sites by distributing them among different hosts. If a computer fails, the next computer steps into the breach.
Flash	Adobe Flash (or simply "Flash", formerly "Macromedia Flash") 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.
Frequency-hopping spread spectrum (FHSS)	The frequency-hopping spread spectrum (FHSS) is a frequency spread process for wireless data transmission. It is divided into fast and slow hopping. The carrier frequency changes, and the sequence of the frequency change is determined by pseudo-random numbers.
FTP	File Transfer Protocol FTP is a network protocol for transferring data via TCP/IP networks. FTP can be used, for instance, to load websites onto a webserver.
General Packet Radio Service (GPRS)	General Packet Radio Service is a packet-oriented service for data transmission that is used in GSM (mobile communication) networks.
Global System for Mobile Communications - Rail(way) (GSM-R)	Global System for Mobile Communications - Rail(way) (GSM-R or GSM-Rail) is a mobile communications system built on the worldwide dominant GSM standard, but modified for use with railways.
Home Location Register (HLR)	The Home Location Register (HLR) is a (distributed) database and central component of a mobile communication network. It is the home register of a mobile number; every registered mobile station and associated mobile communication number is saved in the database.

Information Assurance – Situation in Switzerland and Internationally

IFrame	An IFrame (also inline frame) is an HTML element used to structure websites. It is used to integrate external web contents into one's own website.
Index page	File on a webserver/website that is usually used as the homepage.
Internet Protocol (IP)	The Internet Protocol (IP) is a widespread network protocol in computer networks, constituting the basis of the Internet. It is the implementation of the network layer of the TCP/IP or OSI model.
IP-Address	Address to uniquely identify computers on the Internet or on a TCP/IP-network (e.g.: 172.16.54.87).
JavaScript	An object-based scripting language for developing applications. JavaScripts are programme components integrated in HTML code enabling specific functions in internet browsers. For example, while checking user input on an internet form, a JavaScript can verify that all the characters entered of a telephone number are actually numbers. As is the case with ActiveX Controls, JavaScripts are run on the client's computer. Unfortunately dangerous functions can also be programmed with Javascripts. In contrast to ActiveX, JavaScript is supported by all browsers.
META refreshes	The refresh tag may be used to redirect to another URL when a page is accessed. Using the content parameter, a delay may also be specified before the redirect is executed. For example: <code><meta http-equiv="refresh" content="5; URL=http://www.melani.admin.ch" /></code> This redirects to the website <code>http://www.melani.admin.ch</code> after 5 seconds.
MP3 player	Software or hardware that can play compressed music data files (MP3).
Network-centric warfare (NCW)/ Network-centric operations (NCO)	Network-centric warfare (NCW) is a military concept for war in the information age. Modern IT means are included in warfare. Network-centric operations (NCO) refers to the execution of operations on the basis of network-centric warfare.
P2P	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.
PHP	PHP is a scripting language mainly used to create dynamic websites or web applications.
Referrers	A referrer is the Internet address of the website from which the user has been referred by clicking the link to the current page. The referrer is part of the HTTP query sent to the webserver.
Rogue software. Rogueware	Rogue software, also called rogueware, is malware pretending to have found malicious software (usually spyware) and offering to remove it for a fee.
Rootkit	A collection of programs and technologies which allow unnoticed access to and control of a computer to occur.

Information Assurance – Situation in Switzerland and Internationally

Scareware	Scareware is software designed to scare the user or make the user uncertain. It is an automated form of social engineering. If the victim falls for the trick and believes to be under threat, an offer is often made to the victim to remove the non-existent threat in return for payment. In other cases, the victim is made to believe that an attack has already been successful, causing him or her to perform actions that make the attack possible in the first place.
Security holes	A loophole or bug in hardware or software through which attackers can access a system.
Smart grid	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.
Social networking sites	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.
SCADA systems	Supervisory Control And Data Acquisition Systeme. Are used for monitoring and controlling technical processes (e.g. in energy and water supply).
Time to live (TTL)	Time To Live in the context of the <i>Domain Name System</i> defines how long a record will be cached before it will be retrieved from the authoritative nameserver again.
USB Memory Stick	Small high capacity data storage devices, connected to a computer via the USB interface.
WLAN	WLAN stands for Wireless Local Area Network.
Worm	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 themselves from one computer to another.
Zombie computer	Synonym for bot / malicious bot

7 Annex

7.1 ICANN and OFCOM are looking for solutions in combating fast flux networks

The MELANI semi-annual report 2007/II⁴³ discusses the technical aspects of fast flux networks. In the last two years, the problem has become worse. This has forced ICANN⁴⁴ – the organization responsible for the administration of domain names – to analyze the issue in detail. A first report was published by the ICANN Security and Stability Advisory Committee (SSAC)⁴⁵ in March 2008. The problem confronts ICANN with special challenges, since fast flux networks rely on the use of the DNS via IP (A record with short TTL) and changes to the name server (double fast flux).

In its first report, the SSAC already proposed a first series of solutions to curtail this phenomenon. Notable proposals include deactivating the botnets housing the fast flux infrastructure, deactivating the involved domain names, and limiting changes to name servers.

Based on this report, the Generic Names Supporting Organization (GNSO) of ICANN⁴⁶ published a first report prepared by the Fast Flux Hosting Working Group (FFWG⁴⁷) in January 2009, the final version of which appeared on 6 August 2009⁴⁸.

In part 1 we will analyze the recently published report, and in part 2 we will present the initiatives of other organizations trying to curtail illegal fast flux networks (especially in relation to phishing). Part 3 discusses what Switzerland is doing to adjust its applicable legislation.

Part 1

The GNSO first presents the problem of defining fast flux networks used for illegal purposes (fast flux attack networks) and distinguishing them from volatile networks that can be used for legal purposes. After the interim report in January 2009, ICANN gave Internet users the opportunity to provide feedback on the existing studies. This resulted in interesting inputs, mainly on the part of the most important actors in this field, but also from private citizens. Awareness has grown that various Internet providers are using techniques for their activities that are similar to fast flux networks. These include:

- Organizations administering networks with high attack potential (networks of governments, military installations, but also multinational corporations and significant Internet actors): These networks must be available practically around the clock and use short *TTL* in order to redistribute the requisite resources

⁴³

http://www.melani.admin.ch/dokumentation/00123/00124/01048/index.html?lang=it&download=NHZLpZeg7t,Inp6l0NTU042l2Z6ln1ah2oZn4Z2qZpnO2Yuq2Z6gpJCDdlB7gGym162epYbg2c_JjKbNoKSn6A-- (as of 01.09.2009)

⁴⁴ <http://www.icann.org> (as of 01.02.2009)

⁴⁵ <http://www.icann.org/en/committees/security/sac025.pdf> (as of 01.09.2009)

⁴⁶ <http://gns0.icann.org> (as of 01.09.2009)

⁴⁷ <http://gns0.icann.org/issues/fast-flux-hosting/fast-flux-initial-report-26jan09.pdf> (as of 01.09.2009)

⁴⁸ <http://gns0.icann.org/issues/fast-flux-hosting/fast-flux-final-report-06aug09-en.pdf> (as of 01.09.2009)

Information Assurance – Situation in Switzerland and Internationally

- Distributed networks (such as Akamai): In this case, the volatile networks can distribute the generated data volume to several servers or reduce waiting times by using several servers spread across just as many geographic zones
- Mobility support: Also in this case, short TTL allows the construction of ad hoc networks to support a certain kind of mobility
- Freedom of opinion / interest groups: Bypassing censorship and publication of material that would be impossible otherwise (in addition to fast flux networks, other techniques also exist, such as the Tor network, with the help of which content can be housed at different locations, making it more difficult to identify the computers used, for instance).

These considerations must be made in advance to find out what instruments are best suited to curtail fast flux networks used for criminal purposes. Preventing short TTL, for instance, would damage both criminal and legal fast flux networks. For this reason, the GNSO tried to define the main characteristics of criminal fast flux networks:

- Network nodes may be run on infected computers, but this is not necessarily the case
- They are volatile in that they use a group of bots to achieve this effect
- The botnets are dispersed across several mutually autonomous systems
- The NS (name server) is changed frequently
- The computers' IPs are mainly located in the segment of end users with broadband (ADSL, cable)
- The quality of Whois entries is poor; only little or false information is available regarding the registrant
- The proxy server nginx⁴⁹ is often installed on botnets, which facilitates the creation of a reverse proxy by installing a connection between the victim, the botnet, and the mothership via which the contents circulate (e.g. a website)
- The domain name is registered via an already existing and thus unsuspecting account
- The domain names appear in various number combinations (e.g. as1.com, as2.com, as3.com, etc.)
- The sole purpose of the fast flux network is to prolong the attack (e.g. a phishing attack against a financial institution).

These considerations give rise to two opinions on the best way to curtail illegal fast flux networks. The first recommends information sharing as a countermeasure, while the second would prefer more concrete action on the part of ICANN and its members (registrars and registries⁵⁰). The following ideas were floated to enhance information sharing:

⁴⁹ <http://nginx.net> (as of 01.09.2009)

⁵⁰ "Registries" are organizations responsible for allocating resources for Internet addresses (IP addresses, autonomous systems). "Registrars", by contrast, are responsible for administering domain name reservations.

Information Assurance – Situation in Switzerland and Internationally

- Publish additional, non-sensitive information on domain names that is generated via DNS (and not via Whois). This information could include the age of the domain, the number of changes of the name server over a particular time, and so on.
- Publish summaries of complaints lodged against a domain, listed by registrar, TLD, or name server
- Encourage ISPs to use netflow/sflow to determine whether their clients include botnets
- Promote private initiatives to facilitate information sharing (like the Anti-Phishing Working Group to combat phishing).

But there are also voices calling for more far-reaching measures on the part of ICANN and its members and proposing the following solutions:

- Accelerated procedures for suspending domain names in collaboration with officially accredited agencies
- Guidelines for the use of very low TTL values and limitation of the number of modifications to the same A or NS record that can be made within a defined time period
- Identification of name servers as static or dynamic. For static name servers, the IP address used for the name server should be provided. For dynamic name servers, a premium could be charged.
- A nominal fee for changes to static name servers, split equally between ICANN and the registry. The funds received could be dedicated to abuse handling.
- Improvement of the registration procedure for domain names.

We will see below that some of these methods are already being used in Switzerland or have been circulated for consultations. Others met with a negative response among the affected organizations, however, especially the idea of levying a fee for changes to the name server. This would be counterproductive from a commercial perspective.

At the end of the report, the working group recommends reviewing the following ideas with a view to future developments:

- Identify which of the proposed solutions could be applied through legislation or commercially and which would merely serve to determine best practices
- Evaluate how registrars and registries can best be involved in the policy of shutting down domain names
- Establish a Fast Flux Data Reporting System (FFDRS), i.e. a database to collect information on the fast flux networks
- Make ICANN a facilitator of best practices, aiming for stronger regulation for purposes of curtailing illegal activities
- Explore the possibility of involving other partners in the process of developing measures to combat illegal fast flux networks.

Part 2

Several parts of the final report of the GNSO working group referred to initiatives by other organizations to curtail illegal fast flux networks (especially in the area of phishing). They will be discussed in more detail in the following.

One of the most active groups in this field is without a doubt the Anti-Phishing Working Group (APWG⁵¹). The APWG is an industry association focused on eliminating identity theft and fraudulent phishing attempts via e-mail. In a report published in October 2008⁵², the APWG addressed the registries and gave them recommendations on how to prevent phishing or at least diminish its impact.

According to the APWG, there are various solutions ranging from sensitization of users and complex identification systems to fast methods for shutting down phishing domains and techniques for detecting attempted fraud. The 5 most important recommendations are:

- Short procedures for shutting down domain names, requiring close cooperation between registries and officially accredited agencies
- Proactive use of collected data to identify and shut down domain names used for attacks
- Sharing of domain names used for attacks to law enforcement authorities
- Protection of customers from phishing attempts. As soon as cybercriminals have obtained access data for the domain administration of customers, they can change the DNS of existing domains or reregister them by assuming the unsuspecting identity of a normal customer.⁵³
- Prohibition or limitation of the use of fast flux websites. This includes restrictions on changes to name server names or a minimum number of minutes for TTL.

The APWG report contains a whole series of additional recommendations:

- Once a domain name has been linked to illegal activities, in addition to shutting it down, it should be checked whether the same data (name, IP, e-mail, address, credit card) has been used to register other domain names
- Establish a system for blocking suspicious domain registrations (registrar lock), then collect as much information as possible, from http request headers to the personal data of the registrant. Then try to confirm the collected data: Verify whether domain names exist with similar characteristics (e.g. whether they alternate using a combination of numbers, see above); whether the names contain parts of domain names or well-known trademarks (eBay, PayPal, various financial institutions); examine the IP addresses used to register names and try to confirm them by checking them against the existing black lists (such as Spamhaus XBL); verify authenticity of e-mail addresses; make specification as "fully qualified domain name" (FQDN) mandatory, i.e. declaration of the IP address; verify credit cards used.

⁵¹ <http://www.antiphishing.org> (as of 01.09.2009)

⁵² Anti-Phishing Best Practices Recommendations for Registrars, http://www.antiphishing.org/reports/APWG_RegistrarBestPractices.pdf (as of 01.09.2009)

⁵³ <http://www.icann.org/committees/security/sac028.pdf> (as of 01.09.2009)

Information Assurance – Situation in Switzerland and Internationally

- Then a system could be developed to assign a point system to the data collected, thus allowing screening that is as precise as possible.

The APWG has made many recommendations that require considerable effort and a pronounced will to work together. But the APWG is not the only group pursuing such goals. Other notable initiatives include the Whois Data Problem Reporting Service (WDPRS)⁵⁴. This is a web interface via which users can send notification of incomplete or clearly false Whois domain name data to the registrars belonging to ICANN. These notifications may be initial indications of fraudulent use of the names. Another initiative is Phishtank⁵⁵. This portal can be used by anyone to report phishing e-mails (and the domain names used). The database fed in this way is available to anyone for testing an address and finding out whether it is an already known phishing website. The following three organizations carry out other activities in this field: the Messaging Anti-Abuse Working Group (MAAWG⁵⁶), a working group of the most important actors worldwide involved in electronic messaging services; ShadowServer⁵⁷, which mainly deals with monitoring of botnet activities; and StopBadware⁵⁸, which focuses on creating a database of malware on the Internet.

Part 3

Switzerland has likewise not remained idle. Some legislative amendments were made combating this type of crime possible in the first place. A first step was taken by changing the general registration conditions for domain names ending in ".ch". Until End of February 2009, it was possible to acquire a domain name and use it immediately. An invoice was issued, so that the acquired product could be used for at least 30 days. This made it easy for persons with malicious intent to register the domain name for the duration of a month without having to pay for it. After the month had ended and a payment reminder was sent, the domain name could be cancelled. To prevent this type of abuse, SWITCH changed the conditions of the registration contract⁵⁹. The contract conditions now specify that "the entry in the zonefile generally takes place within 24 hours of processing of the received payment by SWITCH". In other words, the domain name must now first be paid for before it can be used. This first measure proved to be an effective deterrent against mass registration of ".ch" domains, which were used for phishing attempts in 2008.

But that is not all. The Federal Office of Communication (OFCOM) is proposing legislation that will soon be submitted to the political bodies. The proposal envisages a new article in the Ordinance on Addressing Resources in the Telecommunications Sector (AEFV). This article gives SWITCH the possibility of blocking and cancelling a domain name ending in ".ch" if it is suspected of being used for:

- spreading malicious code;
- obtaining sensitive data by way of illegal methods.

The suspicion must be reported to an agency accredited by OFCOM.

⁵⁴ <http://wdprs.internic.net> (as of 01.09.2009)

⁵⁵ <http://www.phishtank.com> (as of 01.09.2009)

⁵⁶ <http://www.maawg.org> (as of 01.09.2009)

⁵⁷ <http://www.shadowserver.org> (as of 01.09.2009)

⁵⁸ <http://www.stopbadware.org> (as of 01.09.2009)

⁵⁹ <https://www.nic.ch/reg/ocView.action?res=EF6GW2JBVPTG67DLNIQXU234MN6SC2T4PAQGM6TDMI#a8> (as of 01.09.2009)

The most important point, which has also been the most controversial in all reports (such as in the APWG and GNSO documents discussed above), was to introduce accelerated procedures allowing the temporary deactivation or complete deletion of a domain name through cooperation between registrars and accredited agencies. With this draft legislation, Switzerland could however make a huge step forward in the fight against Internet crime.

7.2 Browser settings for the protection against common Drive-by infections

Introduction

Every website consists of various instructions, the so-called HTML code. These instructions tell the browser (e.g. Internet Explorer) how to display the content of the website. While some websites only consist of text documents and do not contain additional functions (static sites), other sites contain dynamic content. Examples are tickers, web forms for online ordering, animated images, or dynamically displayed advertising banners. Such dynamic functions can be realized with ActiveX Controls and JavaScript. Unfortunately, these can also be misused to trigger unwanted and damaging actions on the visitor's computer.

General rules:

Regular updates of operating system and applications

Some products make an automatic update function available for this purpose, which you should definitely use. Check regularly whether it is activated. Information on current software updates is generally available on the producer's website.

Restrict JavaScript

Restrict (or disable) the execution of JavaScripts (Active Scripting) as much as possible using the browser settings. When deactivating JavaScript, however, it should be pointed out that many websites will no longer function correctly. Should this interfere with your surfing too much, you can relax the restrictions (step-by-step) to the extent you find acceptable.

Restrict ActiveX Controls (only Internet Explorer)

Restrict the execution of ActiveX Controls as much as possible using the browser settings.

Change the security settings of Internet Explorer to "High". How to do this is described on pages 5 and 6 of the "Security settings for Windows XP" instructions⁶⁰ (these instructions for setting the security level for Internet Explorer are also valid for other Windows operating systems).

Important: Since Active Scripting is used on many websites, certain sites will no longer be fully displayed after changing these settings. For this reason, it is worthwhile to include frequently visited sites (which you trust) in the list of "trusted sites". How to do this is also described on page 6 of the "Security settings for Windows XP" instructions.

Note: Using the high security settings in Internet Explorer automatically disables the following functions (JavaScript, IFrame, and META refresh)

⁶⁰ <http://www.melani.admin.ch/dienstleistungen/00132/00149/index.html?lang=en> (as of: 01.09.2009)

Information Assurance – Situation in Switzerland and Internationally

The following remarks discuss individual threats relating to drive-by infections and propose appropriate countermeasures.

Case 1: Obfuscated (concealed) JavaScript (JavaScript is used in the attempt to redirect the computer to a malicious page)

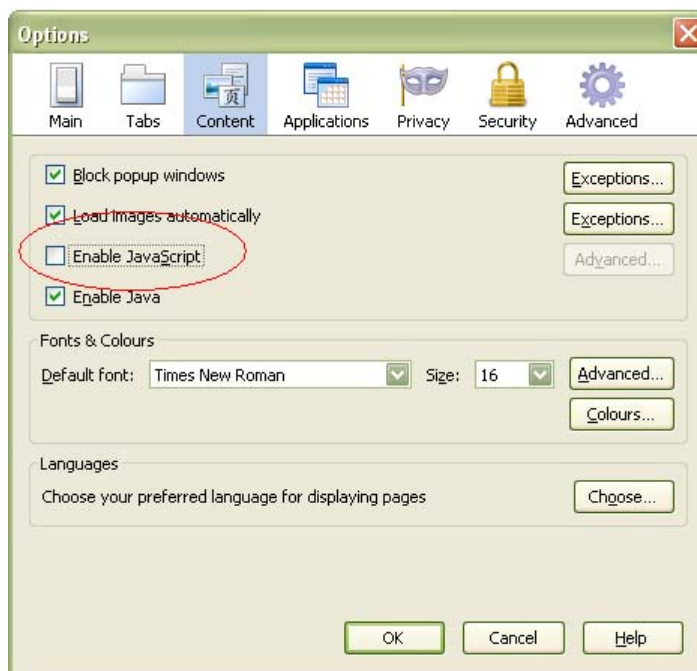
→ Solution: Disable JavaScript

→ Disadvantage: Pages using JavaScript no longer work

Firefox

Option 1: Use the NoScript programme⁶¹. With a simple mouse click, this allows JavaScript to be reactivated permanently or temporarily for individual sites.

Option 2: Tools → Options → Content: Uncheck « Enable JavaScript »

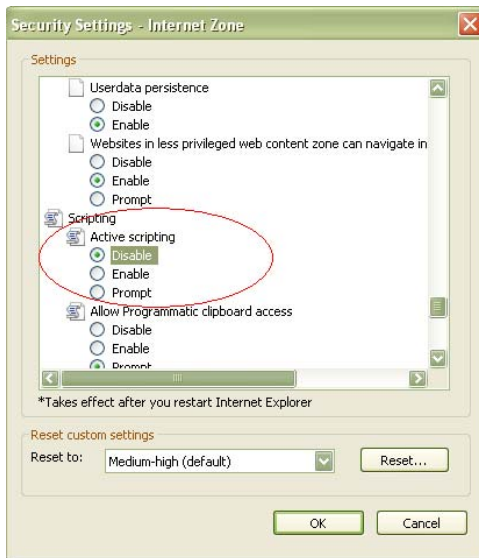


Internet Explorer

Tools → Internet Options → Security → select the level for the Internet zone. Scripting can either be disabled entirely, or the user is asked for every site whether JavaScript should be enabled where applicable (prompt).

⁶¹ <https://addons.mozilla.org/de/firefox/addon/722> (as of: 01.09.2009)

Information Assurance – Situation in Switzerland and Internationally



Case 2: IFrame exploit (By way of an IFrame – page within a page – the browser opens a malicious page in the background)

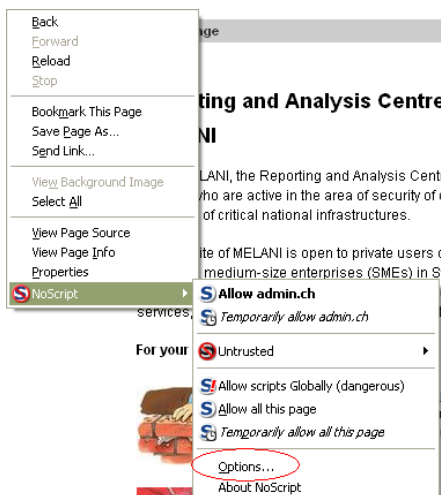
→ Solution: Disable IFrame

→ Disadvantage: Pages requiring iFrames only partially work

Firefox

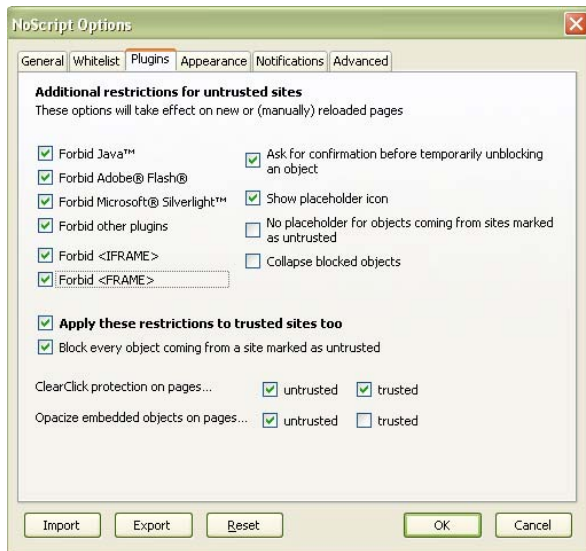
Option 1: Use the NoScript programme

After installing the NoScript programme, click on the right mouse key in the browser, choose NoScript and select the Options menu.



Forbid <IFRAME> and <FRAME>

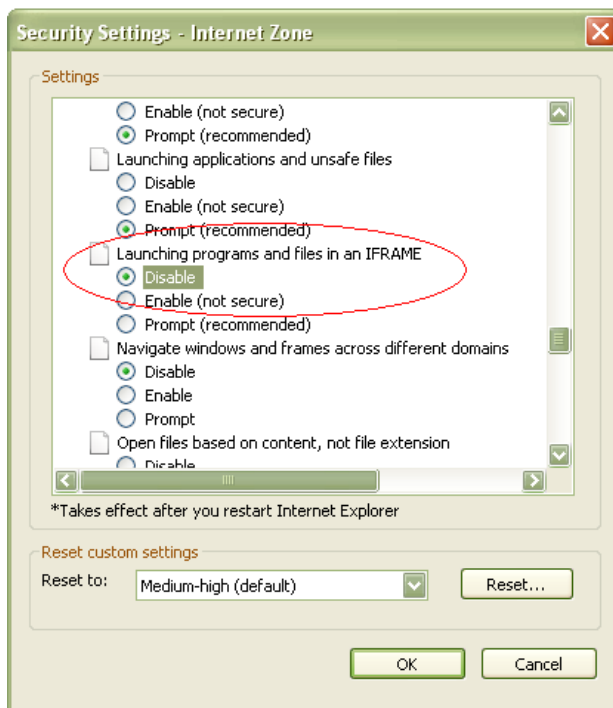
Information Assurance – Situation in Switzerland and Internationally



Option 2: In the address bar of the browser, enter: **About:config** and set the function **Browser.frames.enabled** to **false**.

Internet Explorer

Tools → Internet Options → Security → select the level for the Internet zone. IFrames can either be disabled completely, or the user is asked for every site whether IFrame should be enabled where applicable (prompt).



Case 3: META refresh (The META refresh command automatically redirects the browser to a malicious page)

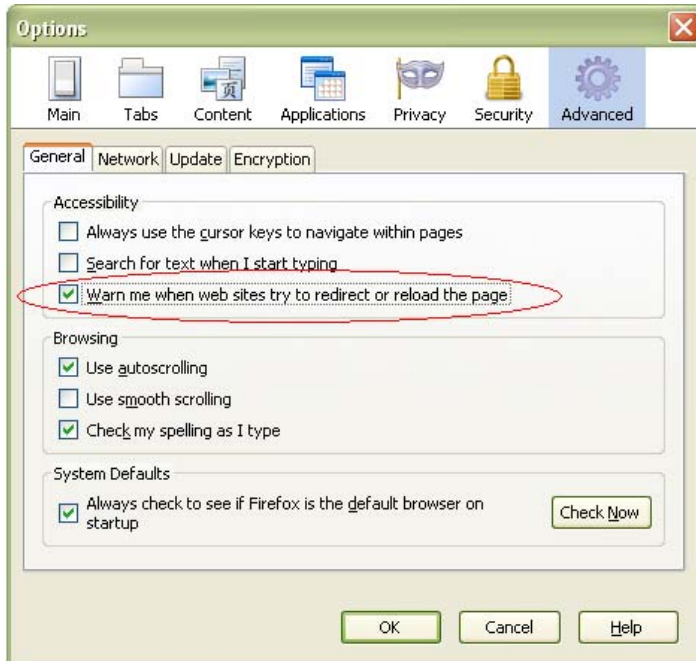
→ Solution: Restrict META refresh

→ Disadvantage: Pages with redirects function only partially.

Information Assurance – Situation in Switzerland and Internationally

Firefox

Tools → Options, "Warn me when web sites try to redirect or reload the page". Every time an attempt is made to redirect the browser, this must be confirmed manually.



Internet Explorer

Tools → Internet Options → Security → select the level for the Internet zone to completely disable META refreshes.

