Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

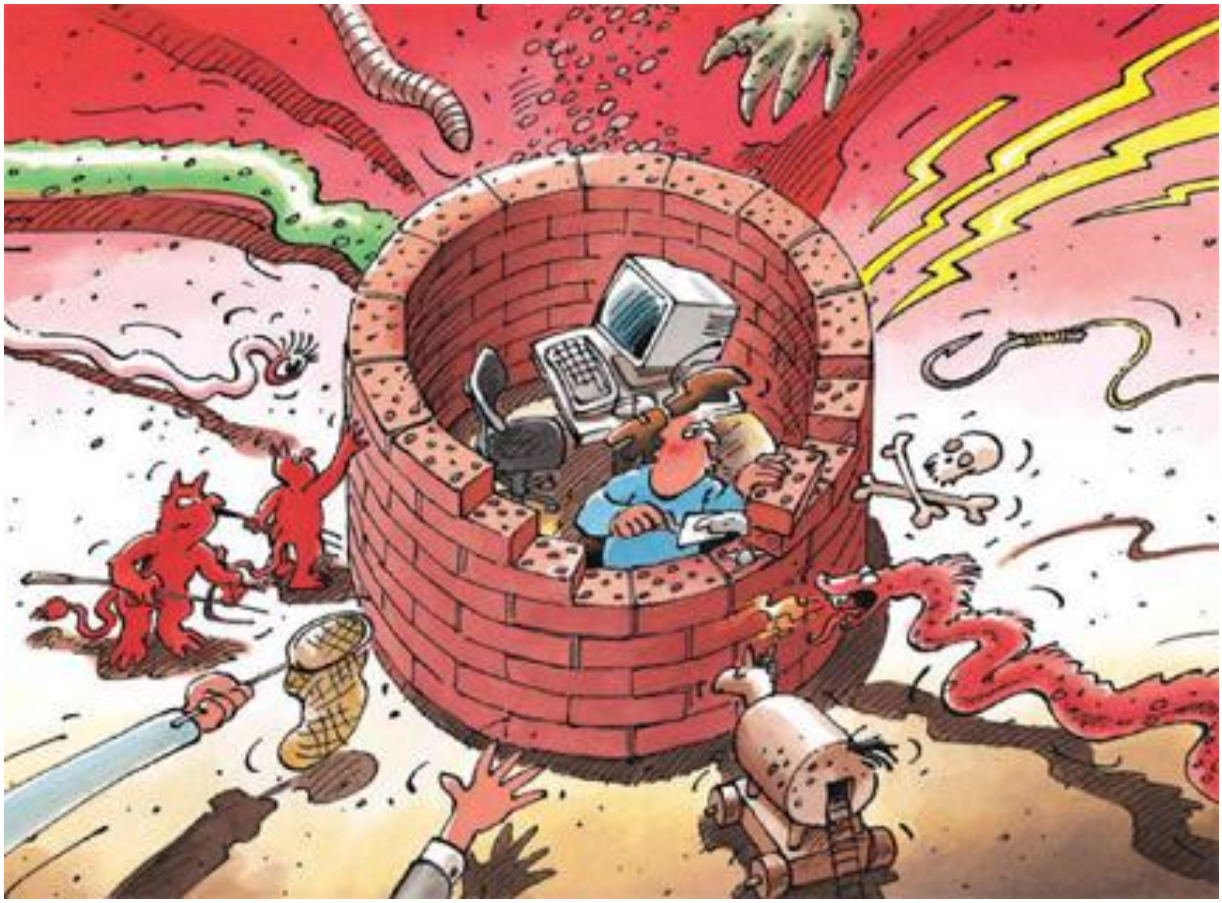
Federal Strategy Unit for IT FSUIT
Federal Office of Police fedpol

Reporting and Analysis Centre for Information Assurance MELANI

Information Assurance

Situation in Switzerland and Internationally

Semi-annual report 2007/II (July – December)



In collaboration with:

KOBIK
SCOCI
CYCO

Koordinationsstelle zur Bekämpfung der Internet-Kriminalität

Le service national de coordination de la lutte contre la criminalité sur Internet

Il Servizio nazionale di coordinazione per la lotta contro la criminalità su Internet

The Swiss Coordination Unit for Cybercrime Control

Contents

Focus areas of issue 2007/II

- **Point of attack: Human/computer interface**
  In the field of information assurance and Internet crime, the focus is increasingly on the significance of the human/computer interface. While technical measures provide basic protection from attacks, they are no longer sufficient on their own.
  ► Current situation: Chapter 2.1
  ► Incidents in Switzerland: Chapter 4.1
  ► International incidents: Chapter 5.2

- **Espionage and data theft**
  The threat of targeted espionage persists, both for government systems and for private companies. Here again, the human/computer interface is significant, since *social engineering* and research prior to an attack are playing an ever-increasing role. This approach permits highly targeted attacks, which are difficult for even very observant persons to detect. More and more, the awareness-raising and sensitization of employees is becoming important, as well as clear guidelines on the use, storage, and availability of information.
  ► Incidents in Switzerland: Chapter 4.1
  ► International incidents: Chapter 5.2

- **Botnets and DDoS attacks**
  Botnets continue to be the most important threat on the Internet. These remote-controlled computers are used for many purposes, including: distribution of *spam*, illegal hosting, information gathering, and *DDoS attacks*. As a rule, the user does not know that his or her computer is part of a botnet. DDoS attacks have been observed in Switzerland as well over the past half year, and it must be assumed that botnets will be used even more in the future.
  ► Current situation: Chapter 2.3
  ► Trends for the next half year: Chapter 3.1
  ► Incidents in Switzerland: Chapter 4.1
  ► International incidents: Chapter 5.2
  ► Appendix: Chapter 10.1

- **Malware / attack vectors**
  Attacks over the past half year have again demonstrated the trend toward modular and flexible *malware*. Malware is put together individually, and contains precisely the functions needed for the attack in question. The trend of distributing malware via *drive-by infections* persists. Weaknesses in web servers and their applications are exploited to infect unsuspicious and heavily trafficked websites. The attacks are often carried out via *vulnerabilities* in web applications.
  ► Current situation: Chapter 2.2
  ► Incidents in Switzerland: Chapter 4.1
  ► Prevention: Chapter 6

1 Introduction

The sixth semi-annual report (July – December 2007) 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** at the end of this report. Comments by MELANI are indicated by a shaded box.

Chapter 2 describes the current situation, threats, and risks of the last half year. **Chapter 3** provides an outlook on the expected developments.

Chapters 4 and 5 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 2007. The reader will find illustrative examples and details supplementing the more general information contained in Chapters 2 and 3.

Chapter 6 discusses a topic in the field of prevention that is closely related to the threats covered in Chapter 2.

Chapter 7 focuses on public and private sector activities relating to information assurance in Switzerland and abroad.

Chapter 8 summarizes changes to the legal foundations.

Chapter 9 contains a glossary with the most important terms used in this report.

Chapter 10 is an appendix with expanded technical explanations and instructions on selected topics covered in the semi-annual report.

2 Current Situation, Threats and Risks

2.1 Point of Attack: Human/Computer Interface

In the field of information assurance and Internet crime, the focus is increasingly on the significance of the human/computer interface. While technical measures provide basic protection from attacks (see Chapter 6), they are no longer sufficient on their own. To successfully defend against attacks, the prudence of the computer user pays an increasingly important role, since attacks may contain *malware* that is not recognized by up-to-date, widely used anti-virus software at the time of the attack. At the same time, increasingly detailed research in advance of an attack and sophisticated *social engineering* permit extremely targeted attacks, making them difficult for even very observant persons to detect.

Every computer is an attractive target for attacks, even if the owner may not suspect it. On the one hand, the data on the computer are of interest, especially those that can be used to make money. This includes personal information such as credit cards, tax and e-banking data, software license keys, and the like. On the other hand, computer performance and bandwidth can be stolen. Computers on which no exploitable data have been stolen can still be integrated into *botnets* and, for instance, abused for the dissemination of *spam* or *DDoS attacks* (see Chapter 3.1).

The dissemination of malware such as by the Storm Worm relies on technical sophistication, but especially also on efficient social engineering (see Chapter 5.2). Such attacks lure computer users into installing malware by successfully pretending to be something different.

The human/computer interface also plays an important role in the persisting espionage attacks (see Chapters 4.1 and 5.2). Using detailed research in advance, attacks are becoming increasingly targeted; the attacker knows what can be obtained where and how. Attackers employ e-mail content adapted to the victim, an attractive link, or a trust-inspiring sender address, so that the attacks appear as unsuspicious as possible and are not identified as malicious. The malware used is often not recognized by the usual anti-virus software. Both targeted research and social engineering play a significant role in this kind of attack.

Technical measures alone offer less and less protection against attacks. Awareness-raising and sensitization of every individual computer user – especially workplace employees – is thus becoming increasingly important, as well as clear guidelines on handling documents and files. Computers are attacked to steal personal data, engage in espionage, distribute malware, or carry out DDoS attacks. Future attacks will increasingly focus on social engineering and, in cases of targeted attacks, improved research of their victims.

2.2 Malware: Infection in Several Steps

The attacks over the past half year have once again demonstrated the trend toward modular and flexible *malware*. Malware is put together individually and contains precisely the

functions needed for the attack in question. The e-banking Trojans[1] appearing in Switzerland, but also the malware attack against the Federal Administration described in Chapter 4.1 show this clearly.

Modern malware usually infects computers in several steps. Flexible and easy-to-use malware kits are employed. A small utility program is used to disseminate the malware, a so-called *downloader*. Downloaders can be adapted using *packers* and *crypters*, so that they are no longer recognized by anti-virus software. The downloader prepares the computer for the actual infection, by deactivating the firewall and the anti-virus software, for instance. This makes things easy for the actual malware, which is then downloaded from a server.

The trend of distributing malware via *drive-by infections* persists. A recently published study by Google confirms a steady increase of websites abused for *drive-by infections*.[2] The Storm Worm (Chapter 5.2), for instance, which initially spread via an e-mail attachment, soon shifted to e-mails with links to bogus websites exploiting *vulnerabilities.*

In particular, vulnerabilities in web servers and their applications are exploited to infect unsuspicious and heavily visited websites with drive-by infections. For this reason, Chapter 6.2 is addressed expressly to website operators and discusses the methods for countering this trend.

On the *client* side, vulnerabilities especially in the browser, add-ons, and applications are exploited. Practically no program is immune from vulnerabilities. As soon as these programs communicate over the Internet or open or play files from the Internet, they are exposed to threats. In the last half year, affected applications other than browsers included FlashPlayer, Acrobat Reader, Apple's QuickTime, and the RealPlayer plug-in, and vulnerabilities were also found in instant messenger and anti-virus programs. It is therefore always essential to update all installed programs. Chapter 6.1 addresses this issue and suggests simple technical measures that can be taken.

Professional and user-friendly tools make it possible for almost anyone to create his or her own malware – if the creator has sufficient criminal energy and is ready to pay the necessary price. The key to success is efficiently placing the malware on the computer of the victim. Exploiting the good faith of the computer user (*social engineering*) and circumventing the security measures of the computer are crucial. Given the countless variations of malware and the high number of associated signatures targeted by anti-software manufacturers, the usual method of signature recognition currently used will likely reach its limits. This can be seen in the decreasing recognition rate of anti-virus software.

It is recommended that website operators keep their web applications up-to-date and that they ensure that the hosting provider also carries out the necessary updates and security measures (Chapter 6.2).

2.3 Botnets

Botnets remain the most serious threat on the Internet. Computers are remote-controlled and secretly integrated into networks, where they are abused for illegal purposes. As a rule, the

[1] For information on the attacks against Swiss financial services, see MELANI semi-annual report 2007/I: http://www.melani.admin.ch/dokumentation/00123/00124/01029/index.html?lang=en (as of: 19.02.2008).

[2] http://googleonlinesecurity.blogspot.com/2008/02/all-your-iframe-are-point-to-us.html (as of: 19.02.2008).

user does not know that his or her computer is part of a botnet. Signs that the computer has become part of a botnet – such as slow performance or frequent crashes – are generally ignored. The owners affected are not aware that their computer has become a small but nevertheless important component of a botnet, potentially allowing a wide range of criminal activities to be perpetrated on the Internet. These include the dissemination of *spam*, hosting of illegal content, gathering of information, *click fraud*, installation of advertising programs, and *DDoS attacks* (see Chapter 3.1). Such services are offered on the underground market and rented out to criminals. Many users are not interested enough in the security of their computers or overestimate their security, and they neglect basic security measures and rules of conduct.

The most infamous botnet in 2007 was the Storm Worm botnet (see Chapter 5.2). This botnet is not steered by a central command-and-control server, but rather is *peer-to-peer*. This technique and the use of fast flux (see Appendix 10.1) make countermeasures harder.

DDoS attacks carried out with the help of a botnet will likely increase in the future (see Chapter 3.1).

Due to efficient *social engineering* in the distribution of *malware* and sophisticated technical methods that make countermeasures difficult, the fight against botnets remains a challenge. The true number of bots is a matter of speculation.

The uncertainty of many Internet users concerning the security of their computer and the threats on the Internet are what make it possible for criminals to develop this type of business model in the first place. Every Internet user should therefore obtain information on preventive measures and an adequate basic protection of his or her computer.[3] This is important in particular because infected computers and computers integrated into botnets can be used for criminal dealings.

3 Trends / General Developments

3.1 DDoS Attacks

As already mentioned in the last chapter, *botnets* are also used for *DDoS attacks*. Recent major known attacks included the DDoS attacks against the Estonian IT infrastructure and the attack against the IT security provider CastleCops.[4] Several DDoS attacks have been observed in Switzerland in the last half year, including against Swisscom and sexy-tipp.ch (see Chapter 4.1).

[3] Protection measures and rules of conduct can be found at: http://www.melani.admin.ch/themen/00166/index.html?lang=en (as of: 22.02.2008).

[4] For the DDoS attack against Estonia, see Chapter 5.1 of MELANI semi-annual report 2007/I: http://www.melani.admin.ch/dokumentation/00123/00124/01029/index.html?lang=en and for the attack on CastleCops: http://www.networkworld.com/news/2007/091207-online-thugs-assault-security-help.html (as of: 15.02.2008).

The focus of DDoS attacks continues to be on securing one's own botnets. Attacks are therefore primarily carried out against rival botnets. However, persons or companies who threaten the functioning of the botnets may also end up in the crossfire. This includes attacks against anti-spam service providers.

In the near future, an increase of DDoS attacks with a political, religious, and especially financial background is expected. The required technical potential is certainly already available. The spectrum ranges from disrupting Internet transactions of a competitor to classic DDoS blackmail. Another trend in DDoS attacks is the use of multipliers. Instead of sending a large number of requests to a web server, DDoS attacks may now also attempt to exploit the weaknesses of a web server to overwhelm it with just a few, manipulated search queries (see Chapter 4.1). Attacks on DNS root servers in February 2007 also showed that a targeted attack on a weak point may increase its probability of success.[5]

3.2 Money Laundering After Phishing

Again in the second half of 2007, there were attacks using *malware* against e-banking systems. The bottleneck in these attacks continues to be the transfer of money abroad. Traditionally, money is transferred abroad by so-called financial agents via Western Union. However, each financial agent can only be used once, since his or her identity is then known to the bank or the prosecutor, and appropriate countermeasures can be taken. Along with the increased awareness of the population, it is becoming increasingly difficult for attackers to recruit financial agents. This is also seen in the financial agent recruiting sites reported to MELANI. While financial agent e-mails and sites were reported to MELANI almost daily in summer 2007, these reports decreased significantly in winter 2007.

The attackers are reacting by improving their selection process in the recruitment of financial agents (see Chapter 5.2) and by shifting to other countries. But also many other European countries are on track with respect to sensitization and prosecution of financial agents. However, a new development could be triggered by the Single Euro Payments Area (SEPA, see Chapter 8), which will make cross-border euro payments faster and cheaper. In particular, cross-border transfers must be as fast by 2012 as national transfers. This could open up a new financial agent market, since countries are included in this zone in which potential perpetrators of e-banking offences are suspected.

Money launderers are forced to find more efficient ways of recruiting so-called “money mules” and to make their offers look more credible. The targeting of clients of online job markets in Chapter 5.2 demonstrates this. MELANI also expects the emergence of new methods that will be even more difficult to recognize as money laundering. One known variation is the direct payment of cars and hotel rooms with assets stemming from *phishing*. The payment is then cancelled, and the money is transferred back to a fictitious beneficiary via Western Union. MELANI has already drawn attention to this type of money laundering in the past.[6] Another example is the establishment of fictitious donor organizations looking for gullible persons as "donation managers", for the ostensible purpose of transferring the money to aid projects in Eastern Europe.

[5] For the attacks against DNS root servers, see also Chapter 5.1 of MELANI semi-annual report 2007/I: http://www.melani.admin.ch/dokumentation/00123/00124/01029/index.html?lang=en (as of: 15.02.2008).

[6] See the following MELANI notice: http://www.melani.admin.ch/dienstleistungen/archiv/01015/index.html?lang=en (as of: 15.02.2008).

3.3 Mobile Phones as Targets?

Are mobile phones a target for criminals? The proliferation of smartphones and mobile phones with computer-like functions, along with the storage of sensitive data on such devices, makes this question unavoidable. A healthy degree of scepticism is appropriate with respect to exaggerated claims of such threats, especially given the commercial interests of some security firms. Nevertheless: It is a fact that the ongoing development and dissemination of modern mobile devices has led to new attack vectors.

The first known smartphone virus was the Cabir worm, which spread via the Bluetooth interface in 2004. Other than resulting in empty batteries, since it was constantly looking for discoverable Bluetooth devices, it did not cause major damage. More problematic is that pests exist which, for instance, autonomously send expensive MMS messages, destroy data, or make phones unusable.[7]

Some manufacturers of anti-virus programs believe the threat potential of mobile phone viruses to be high.[8] The number of cases of actual *malware* attacks on mobile phones remains relatively low, however.[9] A recent survey by IT anti-virus specialist G Data argues that the virus threat for smartphones is low, since smartphones are not a worthwhile target for the malware industry. Reasons include the high number of operating systems, the difficult distribution of malware, and the lack of "computer crime business models". Until now, malware has often been distributed by Bluetooth or MMS. Bluetooth is not suitable for rapid distribution, however, and the installation of malware distributed by MMS requires a user action. A theoretical danger consists of surfing websites infected by *drive-by infections*, as is the case for personal computers.[10]

The attractiveness of mobile phones as a target for malware attacks and data theft is determined by at least two factors: First, the more mobile phones perform the same functions as personal computers (Internet access, storage of sensitive data, performance of financial transactions, etc.), the more they become a lucrative target for criminals. Second, similarly to malware targeting personal computers, it can be assumed that mobile phone malware will become more attractive as the size of the "target audience" grows. It can therefore be expected that modern mobile phones will become an increasingly attractive target as they become more widespread. These developments will cause similar problems in the mobile world as on the Internet.

[7] For an analysis of the development of mobile pests, see: http://www.cs.virginia.edu/~robins/Malware_Goes_Mobile.pdf (as of: 13.02.2008).

[8] See, e.g., the following study published by McAfee: http://www.mcafee.com/de/about/press/corporate/2007/20070212_174646_p.html (as of: 13.02.2008).

[9] See http://www.computerworld.ch/aktuell/itsecurity/41264/index.html (as of: 13.02.2008).

[10] For the G Data survey, see: http://www.gdata.de/unternehmen/DE/articleview/3988/1/160/ (as of: 13.02.2008).

4 Current National ICT Infrastructure Situation

4.1 Attacks

Targeted Malware Attack Against Computers of the Federal Administration

Several times already, MELANI has drawn attention to the danger of espionage by means of *malware*. From the end of November to the beginning of December 2007, the Federal Administration was attacked. In two waves, a total of more than 500 e-mails were sent to employees of the Federal Administration. The e-mail messages were personalized, i.e. the correct form of address of the recipient was used. The bogus sender was a federal office providing information on a supposed photo contest. To participate in the contest, the recipient was called upon to click on a link contained in the e-mail message. Clicking on the link opened a convincing copy of the website of that federal office; the copy had been set up on the server of an Internet service provider in an African country. Under the heading "photo contest", several photographs were displayed. Visitors could vote for a picture by clicking on it. This caused a screensaver file to be downloaded to the user's computer, containing malware. At the time of the incident, the malware was not recognized by commonly-used virus scanners.

GovCERT.ch, part of the Federal Strategy Unit for IT, which will take over the role of MELANI's Computer Emergency Response Team (CERT) on 1 April 2008, examined the malware in detail. The analysis of the program code and the evaluation of the malware's behaviour showed that it was a *Trojan horse*, downloading and executing espionage programs from several computers on the Internet over a defined timeframe. At the time this semi-annual report was compiled, further investigations were underway.

The preparation of the attack, the programming of the malware, and the way it attempted to make analysis more difficult indicate that it was distributed by professional perpetrators with considerable financial and technical resources.

At the time, the malware was not recognized by the usual anti-virus software. It hid inside running processes, some of which are always active. It also used ports for communication with servers on the Internet that are hardly blocked by network gateways (e.g. firewalls).

Technical measures alone can hardly prevent targeted espionage attacks. All the more important is awareness-raising and sensitization of staff members, as well as clear guidelines on the use, storage, and available of information. In the case of the photo contest, the malicious software could only be installed because staff members were lured into participating in the (bogus) contest and into clicking on links. Such social engineering techniques will become increasingly important in the future, especially given that the protection of operating systems against the automatic installation of malware is becoming better all the time.

Attack on parlament.ch

The availability of the website of the Swiss parliamentary services (parlament.ch) was adversely affected from 14 to 18 December 2007. In short intervals, search queries generating long result lists were submitted to the database of the content management system (CMS), which retarded the response time of the server. The queries were submitted by anonymized *IP addresses*.

The motivation for these queries in unclear. Once the search queries were restricted, the stability of the system was re-established.

This attack shows that the number of queries must not necessarily be large to affect the availability of a site. In this case, it was sufficient to manipulate the search queries so that even just a few queries could retard the response time of the server. In general, consistent input validation – i.e. verification of the information typed in – should play an important role in the case of interactive web content.

DDoS Attacks in Switzerland

From 9 August 2007 to 12 December 2007, the website www.sexy-tipp.ch was attacked by a botnet. The portal of the website has been accessible again since the middle of December, but the forum with its more than 50,000 visitors, which was targeted by the attackers, is still not online, even though the owners have already switched providers several times.[11]

Sexy-tipp.ch is not the only website for adults that has become a target of such attacks, however. Other websites associated with the Zurich brothel scene suffered the same fate. The website of Club 79 was also targeted by DDoS attacks. The site experienced continuous difficulties, even after it switched to an American provider.[12]

Swisscom was also a victim of DDoS attacks. On 21 November 2007, a major attack was launched on the infrastructures of IP-Plus.[13] According to Swisscom spokesman Christian Neuhaus, nearly 3,500 clients felt the impact of this action, including Bluewin and Tamedia. During this time, the online version of the Tages-Anzeiger newspaper was no longer available.[14]

4.2 Crime

Drive-by-infection via .ch Domain

In the second half year of 2007, MELANI registered .ch websites with signs of *drive-by infections*. As in the case of Italy, which MELANI reported on in its last semi-annual report,[15] many of the websites registered in Switzerland were respectable sites.

The Honeynet Project published a study of this type of attack in August 2007 describing the typologies of the infected websites found.[16] The 300,000 registered sites are divided into several categories:

---

[11] As of: 15.12.2007

[12] http://www.sonntagszeitung.ch/nachrichten/artikel-detailseiten/?newsid=4168 (as of: 04.02.2008).

[13] http://www.ip-plus.ch (as of: 26.11.2007).

[14] http://www.tages-anzeiger.ch, "Erfolgreicher Hacker-Angriff auf Swisscom", (published 22.11.2007).

[15] See MELANI semi-annual report 2007/I, Chapter 5.1: http://www.melani.admin.ch/dokumentation/00123/00124/01029/index.html?lang=en (as of: 04.02.2008).

- According to type of content (for adults, music, news, user-generated content such as blogs and warez, i.e. sites on which pirated copies of software are offered);
- Sponsored links that appear in the Google search engine results page that lead to vulnerable webservers;
- Sponsored links encountered on the Google search engine results page (with the help of http://googspy.com);
- Typo *squatter* URLs (the 500 most popular sites from http://alexa.com);
- URLs distributed by spam (from the spam archive http://untroubled.org/spam)

The analysis by the Honeynet Project showed that a total of 306 URLs were infected, which corresponds to 1% of the investigated addresses. In almost 60% of the cases, the URLs contained content for adults. In second place (17%) was the category of URLs contained in spam e-mails. Although infections tended to focus on the more popular websites, in order to infect as high a number of computers as possible, the analysis showed that especially these two categories exposed Internet users to the greatest risks.

Phishing via .ch Domain

Classic *phishing*, i.e. the theft of login data and passwords with the help of bogus bank websites, is disappearing in Switzerland. In other countries like England, however, classic phishing continues to be one of the most popular methods for stealing sensitive data from Internet users. In the second half of 2007, Switzerland was targeted by a criminal organization, which registered hundreds of .ch domain names and loaded them with phishing websites. The phishing attacks were directed against English financial institutions.

Domain names ending in .ch are administered by the Switch foundation[17]. The Switch registration procedure allows criminals to buy URLs that are immediately made available. As soon as the payment is processed (generally with stolen credit cards), the domain name is activated and ready for use. If the payment is not accepted by Switch, because the credit card has been blocked or for any other reason, an administrative procedure is initiated, which may take several months.

To combat this practice, which causes damage to Switch (provision of unpaid services), undermines the image of Switzerland, and ultimately also damages the English financial institutions, Switch and the Swiss Coordination Unit for Cybercrime Control (CYCO)[18] concluded a cooperation agreement. When the Coordination Unit suspects that a particular domain is used solely for criminal purposes, it reports this to Switch, which blocks the site. Thanks to this practice, MELANI and CYCO have recorded a significant decline in phishing cases via Swiss domains.

---

[16] http://honeynet.org/papers/kye.html (as of: 04.02.2008).

[17] http://www.switch.ch (as of: 04.02.2008).

[18] http://www.kobik.ch/index.php?language=en Swiss Coordination Unit for Cybercrime Control (as of: 04.02.2008).

Unauthorized Access to A PABX in Geneva: Fraudulent Use of Telephone Lines

The fraudulent use of telephone lines in Switzerland is not a new phenomenon, but it continues to preoccupy law enforcement authorities. Individual cases have already been mentioned in previous years; in this report, MELANI will discuss a case of unauthorized access that occurred in Geneva between July and September 2007.

In this case, the scammers used special software to recognize the tonality of a telephone line connected with an answering machine. As soon as such a line is recognized, a software program searches the telephone exchange for vulnerabilities. If a vulnerability is found, the criminals use the network to forward their calls. This means that a long-distance call is forwarded through the attacked company, which pays for the cost of the call.

Hackers who succeed in using third-party telephone lines sell call minutes for long-distance calls via "low cost" telephone companies. The costs for these calls are cheaper than any imaginable competition. If a customer wants to call Pakistan, for instance, the telephone company pays for the connection between its location and the tapped PABX – e.g. between Holland and Switzerland – while the rest of the call is charged to the defrauded company.

5 Current International ICT Situation

5.1 Breakdowns

Breakdown of Popular VoIP Software Skype: Service Outage For More Than 24 Hours

The *VoIP* service Skype was massively disrupted for two days starting 16 August 2007. Connecting with the Skype network was only sporadically possible, if at all. According to Skype, the VoIP services crashed due to the routine Microsoft Update on 14 August 2007 and the subsequent reboot[19]. This triggered a major restart reaction for a limited period of time, which affected Skype network resources. A lack of *P2P* network resources aggravated the problem. According to Skype, the normally functional self-healing routines failed because of a software error. However, this is unlikely to have been the sole reason, since such reboots are regularly carried out after a Microsoft Patch Day and had not caused any comparable problems up to that point. Skype therefore added, one day later, that in the case of this Microsoft Update, several unusual factors converged, causing the crash. The boot process not of the clients, but of the *supernodes* and their especially high strain had overwhelmed the otherwise smoothly functioning self-healing process.[20] It remains unclear, however, why the reboot only had this serious impact two days after the Microsoft Update. Rumours that the breakdown was due to a *DDoS attack* were repeatedly and vehemently denied by Skype.

[19] http://heartbeat.skype.com/2007/08/what_happened_on_august_16.html (as of: 18.2.2008).
[20] http://heartbeat.skype.com/2007/08/the_microsoft_connection_explained.html (as of: 18.2.2008).

Although Skype is a proprietary VoIP system, this breakdown triggered a renewed discussion on the reliability of VoIP services. While "normal" telephones are probably the most reliable of all electronic means of communication and even work if there is an electricity outage, many people are not used to means of communication breaking down for hours or even days. In the case of private persons, this may be somewhat bearable – unless they have to call the fire department or an ambulance, for instance. But in the case of companies relying on VoIP, such a breakdown can represent an existential threat. This is also the reason why many companies are hesitating to switch to VoIP. One well-known example is UBS, which recently decided not to switch to VoIP yet.[21] In general, potential switchers to VoIP still look more closely at resistance to breakdowns than at considerations of wiretapping and manipulation.

United Kingdom: Loss of CD-ROM leads to exposure of up to 25 Million sensitive datasets

Within just a few weeks in the second half of 2007, several data losses occurred in the United Kingdom. The losses were not caused by infiltrated *Trojan horses* or hacked systems, but rather by lost data carriers (CDs, laptops).

Two CDs with confidential and personal data of more than 25 million British citizens were lost on 18 October 2007. The data concerned more than 7.25 million British families receiving children's allowances. The data include names, addresses, dates of birth, national insurance numbers, and some bank account information.[22] This loss occurred because the CDs were sent for data verification to the National Audit Office without observing the required security measures. The internal postal system was used. The two CDs never reached their intended recipient and can no longer be found. So far, however, there are no indications that the data has fallen into the wrong hands.

Another case became public the middle of December 2007. Data carriers with names, addresses, and telephone numbers of more than three million student drivers could no longer be found. The US company evaluating the driving tests on behalf of the British authorities was responsible for the loss of the data carrier.[23]

A third case concerned the British Department of Health: A CD with information on 160,000 sick children became lost en route to a large London clinic. In addition, more than 10,000 datasets of adult patients in a total of nine regional areas of the public health system went missing. The various data losses put the government of Prime Minister Gordon Brown under pressure.

Such losses of data are not a new phenomenon, but they now increasingly appear to come to the attention of the public. These examples show that adequate security measures must not only be taken when sending information via the Internet, but also when sending physical data carriers such as USB sticks, CD-ROMs, backup tapes, or other storage media. Not only do technical security measures need to be taken, but also measures targeting the storage, exchange, and availability of information.

---

[21] http://www.inside-it.ch/frontend/insideit?_d=_article&news.id=12590 (as of: 18.2.2008).

[22] http://news.bbc.co.uk/2/hi/uk_news/politics/7103828.stm (as of: 21.02.2008).

[23] http://www.spiegel.de/politik/ausland/0,1518,523948,00.html (as of: 21.02.2008).

Sensitive data must always be encrypted sufficiently for purposes of transfer. Data on notebooks, smartphones, and PDAs must also be encrypted. Although most laptop thieves are not primarily interested in data, but rather on reselling the hardware, the unencrypted storage of data on mobile computers is negligent. In particular, victims are left with an uneasy feeling if they do not know what happens with their data. In the case of particularly sensitive data such as personal data, the Data Protection Act demands that they be protected by technical and organizational measures against unauthorized access.

5.2 Attacks

Targeted Espionage Attacks Persist – Attacks against Rolls Royce and Royal Dutch Shell

Targeted espionage, both on government systems and on private companies, continues to be a major topic in the second half of 2007 and has become even more politically sensitive.[24] Also in Switzerland, targeted espionage attacks on the Federal Administration have taken place (see Chapter 4.1). In countries such as the United States, Germany, the United Kingdom, France, but also India, New Zealand, and Australia, the topic is increasingly being discussed in the media as well as at the political and official level. The media, but also government organizations in some of these countries, suspect an involvement of the Chinese government in some of the espionage attacks. The Chinese government itself rejects these accusations and calls itself a victim of international Internet espionage.[25]

At the beginning of December 2007, the British security service MI5 warned about 300 British companies of electronic attacks allegedly supported by Chinese government organizations.[26] Shortly afterward, it was announced that the Rolls Royce and Royal Dutch Shell companies had become victims of Internet espionage, allegedly on the order of the Chinese government.[27]

Espionage attacks are based on political, military, and economic interests. The attackers may be supported by the State, or they may also be individual or organized actors. Government systems, especially information concerning defence and foreign policy, are

[24] On espionage with targeted malware in the first half of 2007, see MELANI semi-annual report 2007/I, Chapter 2.3: http://www.melani.admin.ch/dokumentation/00123/00124/01029/index.html?lang=en (as of: 13.02.2008).
[25] For information and perspectives on the attacks on the German government, see: http://www.spiegel.de/netzwelt/tech/0,1518,501954,00.html; http://www.spiegel.de/netzwelt/web/0,1518,512914,00.html, in the US: http://www.ft.com/cms/s/0/9dba9ba2-5a3b-11dc-9bcd-0000779fd2ac.html; http://www.uscc.gov/annual_report/2007/report_to_congress.pdf, in the UK: http://www.guardian.co.uk/technology/2007/sep/04/news.internet, in France: http://www.theregister.co.uk/2007/09/12/french_cyberattacks/, in China: http://www.washingtonpost.com/wp-dyn/content/article/2007/09/12/AR2007091200791.html; http://www.spiegel.de/netzwelt/web/0,1518,505462,00.html, for more information on this topic, see also: http://www.securityfocus.com/news/11485 and http://www.mcafee.com/us/local_content/reports/mcafee_criminology_report2007_de.pdf (as of: 13.02.2008).
[26] http://business.timesonline.co.uk/tol/business/industry_sectors/technology/article2980250.ece (as of: 15.02.2008).
[27] http://business.timesonline.co.uk/tol/business/markets/china/article2988228.ece (as of: 15.02.2008).

frequent targets of the attackers. Private companies with knowledge of technical or strategic interest may also be targets, as the attacks on Rolls Royce and Royal Dutch Shell show.

It is very difficult to trace attacks back to specific perpetrators, however, since the perpetrators use numerous servers and *botnets* to cover their tracks. It is therefore even more difficult to distinguish State-sponsored attackers from other attackers operating from the same region. In general, it is important to remember that espionage is a widespread method around the world to obtain information, and that many different countries are likely engaged in espionage. The British security service MI5 estimates that at least 20 foreign intelligence agencies are engaged in activities aimed at espionage in the United Kingdom or against British interests.[28]

With respect to the approach taken in espionage attacks, *social engineering* and advance research on the target play an increasingly important role. These methods allow very targeted attacks, which make it difficult to recognize the attack as such, even on the part of very observant persons. An increase in such targeted attacks has been observed, especially against company executives.[29] The necessary information on the persons in question (e-mail address, function, etc.) needed by the phishers to perform such targeted attacks is often readily accessible on the Internet.[30]

Malware: Data Theft and Targeting of Online Job Market Clients

In August 2007, it became public that a *Trojan* allegedly used stolen employer login data to obtain personal information of jobseekers on Monster.com. By accessing the areas reserved for job posters, the Trojan obtained the data of numerous jobseekers. The stolen data were transmitted to a server containing allegedly more than 1.6 million personal entries. With the stolen data, the thieves intended to recruit helpers for money laundering and to send more personalized *spam* e-mails.[31]

With respect to money laundering, the perpetrators took the following approach: With personally addressed e-mail, they looked for "transfer managers" who would make their accounts available to redirect funds. The stolen funds, which were to be "laundered", were acquired by phishing or other methods. The Trojan was used to send these targeted e-mails. The e-mail was personally addressed to the recipient, and it was clear that the person was looking for a job. The e-mails were very professional and sent in the name of Monster.com or Careerbuilder.com.[32]

Moreover, a connection was discovered between this Trojan and *malware* used for blackmail. E-mails were sent in the name of Monster.com containing personal data of the recipient. The e-mails requested the reader to download a search engine for jobseekers. In actuality, however, the program was malware used for blackmail, so-called *ransomware*,

[28] http://www.mi5.gov.uk/output/Page20.html (as of: 13.02.2008).

[29] See the following message by MessageLabs: http://www.messagelabs.co.uk/resources/news/6592 (as of: 13.02.2008).

[30] For additional information on targeted attacks against executives, see: http://www.networkworld.com/news/2007/111407-whaling.html and http://www.darkreading.com/document.asp?doc_id=134229 (as of: 13.02.2008).

[31] See: http://www.symantec.com/enterprise/security_response/weblog/2007/08/a_monster_trojan.html (as of: 13.02.2008).

[32] See: http://www.symantec.com/enterprise/security_response/weblog/2007/08/post_3.html (as of: 13.02.2008).

which encrypted data on the user's hard drive, in order to blackmail the victim by demanding money in return for decryption.[33]

With respect to aiding and abetting money laundering, one's own account should never be made available for redirecting money from third parties. In the future, such fraudulent offers – in addition to other sophisticated variations (see Chapter 3.2) – will likely occur increasingly frequently in connection with stolen personal data generated by targeted attacks. This allows criminals to more efficiently search for *"money mules"* for purposes of money laundering and to make their offers looks more credible.

To protect one's identity, one should only provide limited personal data on the Internet. Sensitive data (bank accounts, passport numbers, etc.) should never be given to a potential employer, until the seriousness of the offer can be verified.

Botnets: Example of Storm

No other worm has caused as much of a stir in the media recently as the Storm Worm. It is characterized not only by its sophisticated technique, but also by the efficient and diverse social engineering it uses for distribution. The distributed e-mails mainly take advantage of the reader's curiosity and respond to current events, but also holidays such as Christmas, New Year's, Halloween, and Valentine's Day. The topicality causes many people to click on the link in the e-mail, even if they actually know that they should always be careful when receiving an e-mail message from an unknown sender. Once the victim has clicked on the link, he or she is redirected to a website containing a link to *malware*, which may be concealed as a game or video. Such sites also contain *drive-by infections*, which are executed in a targeted manner, depending on the browser and the operating system. The sites generally look unsuspicious and contain the expected contents. Once the user has been infected, no drive-by infection is carried out if the same website is visited again. This serves to minimize users' suspicions, e.g. if the browser crashes, so that the malware can continue to spread undetected. Continuous minor modifications of the malware also make it more difficult for anti-virus software to detect. The infected computer is then integrated into a *botnet*. This botnet is not controlled by a central command-and-control server, but rather on a *peer-to-peer* basis. A *rootkit* function is also contained in the Storm Worm. The computer may then be controlled and used by the botnet owner for any imaginable purpose.

The estimates of the size of the Storm botnet diverge widely, ranging from 40,000[34] to several million[35]. The inclusion of the Storm Worm in Microsoft's Malicious Software Removal Tool in September 2007 certainly reduced the size of the botnet significantly.[36] Currently, the Storm Worm is primarily responsible for spam waves, not for *DDoS attacks.* The registered DDoS attacks by Storm were primarily directed at security software companies attempting to discover the command and operation structure of Storm.[37] It can be assumed that the operators or owners of the botnet rent it out to interested persons and are prepared to accept

[33] See: http://www.symantec.com/enterprise/security_response/weblog/2007/08/a_monster_trojan.html; http://www.heise.de/security/news/meldung/94570 and

[34] http://honeyblog.org/archives/156-Measuring-the-Success-Rate-of-Storm-Worm.html (as of: 11.2.2008).

[35] http://www.informationweek.com/news/showArticle.jhtml?articleID=201500196 (as of: 11.2.2008).

[36] http://arstechnica.com/news.ars/post/20071025-storm-worm-going-out-with-a-bang-mounts-ddos-attacks-against-researchers.html (as of: 11.2.2008).

[37] http://www.tecchannel.de/sicherheit/news/1737125/ (as of: 11.2.2008).

any type of order (including DDoS attacks). For instance, there are indications that the network is being rented out to phishers.[38] A description of the *P2P* structure on which the Storm Worm is based can be found in Annex 10.1. For an assessment of the development and threat of botnets, see Chapter 2.3.

USA: One Click of A Mouse Could Plunge A City into Darkness (SCADA Penetration Test in the Idaho National Laboratory)

The supervision and control of industrial facilities (chemicals, power plants, automobile industry, etc.), distribution systems for essential goods (electricity, water, fuel, etc.) and transport and traffic (railways, traffic management systems, postal service, etc.) has long been inconceivable without the use of information and communication technologies (ICT). The development and operation of "Supervisory Control and Data Acquisition (SCADA)" systems has a long tradition.

Originally, SCADA systems were only superficially similar to traditional ICT; they were isolated from computer networks, used proprietary hardware and software, and employed their own protocols to communicate with the central computer.[39] The wide availability of relatively inexpensive devices with built-in interfaces to the Internet protocol has brought about significant changes in this area in recent years. Thermometers, pressure gauges, pumps, switches, and other field elements nowadays often have their own IP address and use TCP/IP to communicate with the central computer. The advantage of using low-cost traditional ICT is balanced by the fact that SCADA systems now are in principle exposed to the same threats that we know from the Internet – *malware* (viruses, worms, etc.) and attackers (hackers) are let in.

In September, CNN reported on an experiment conducted at the Idaho National Laboratory of the U.S. Department of Energy.[40] The experiment showed how a computer-assisted attack on a control system could lead to the physical destruction of an electricity generator. A video showed how the generator begins to shake and smoke before grinding to a complete halt. Headlines were circulated such as "one click of a mouse could plunge an entire city into darkness".

The experiment of the Idaho National Laboratory should be considered a feasibility study. Various factors, such as the type of the employed *relays*, switch configurations, IT security measures, etc., currently make such attacks on electricity providers in Europe very unlikely. However, one should be aware that the conversion to numeric relays is progressing, and economic pressure will increasingly entail that no longer simply individual relays, but rather entire substations will be remote-controlled and operated without staff. Moreover, the consistent use of the same network technology facilitates the desire of management to link the business network and the control network. Data and information on production can thus be viewed directly by management, and production can even be directed by management. This "from shop-floor to top-floor" mentality will pose greater challenges for ICT security in the future. The goal is to prevent incidents, such as the introduction of viruses into the

[38] http://blog.trendmicro.com/2008/01/08/ (as of: 11.2.2008).

[39] For detailed literature, see http://www.industrialdefender.com/general_downloads/nist/nist-sp-800-82_draft.pdf (as of: 30.1.2008).

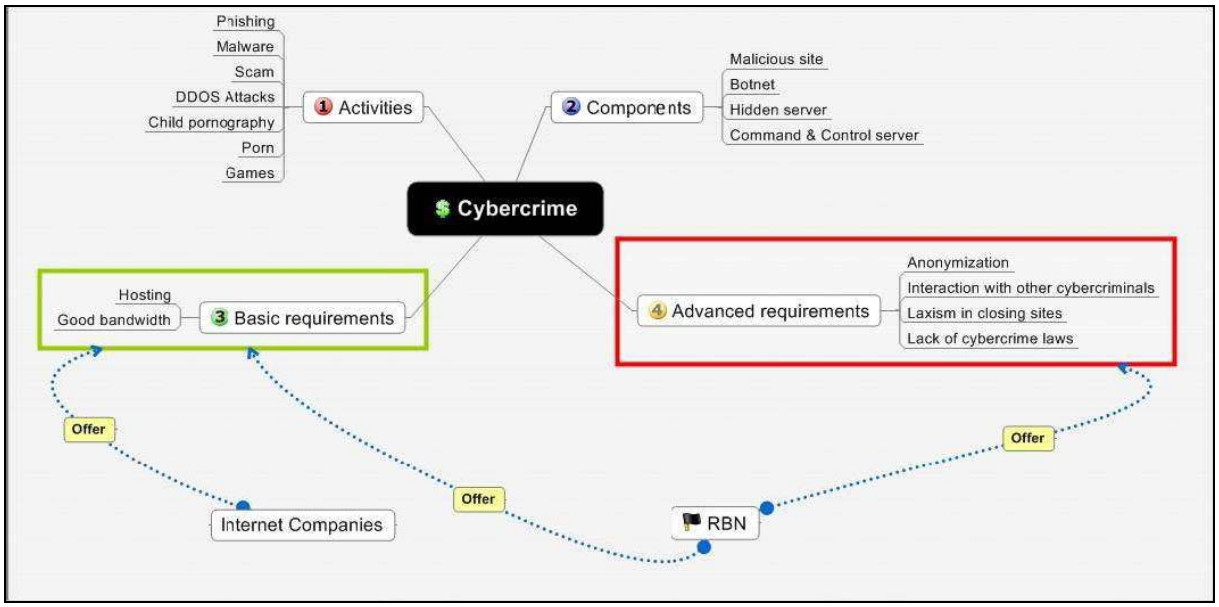
[40] http://edition.cnn.com/2007/US/09/27/power.at.risk/index.html (as of: 30.1.2008).

company network, from spreading to the control network. It will therefore be indispensable to apply principles of traditional ICT security (such as "in-depth defence") or corresponding standards and guidelines to control systems as well. A comprehensive package of measures also includes the exchange of experiences among operators of control systems (e.g. concerning vulnerabilities) and between operators and the authorities, who may be able to contribute information on the current threat situation. MELANI is in close contact with Swiss electricity providers and participates in international information exchanges, such as within the framework of the European SCADA and Control Systems Information Exchange (EuroSCSIE).

5.3 Crime

Frequent Source of Computer Crime: The Russian Business Network (RBN)

The Russian Business Network (RBN) is a Russian Internet service provider (ISP). It has gained notoriety as one of the most popular providers of services for computer crime. To better understand the functions of RBN in the world of computer crime, see the following diagram[41]:



RBN offers a complete infrastructure for carrying out illegal activities, for instance:

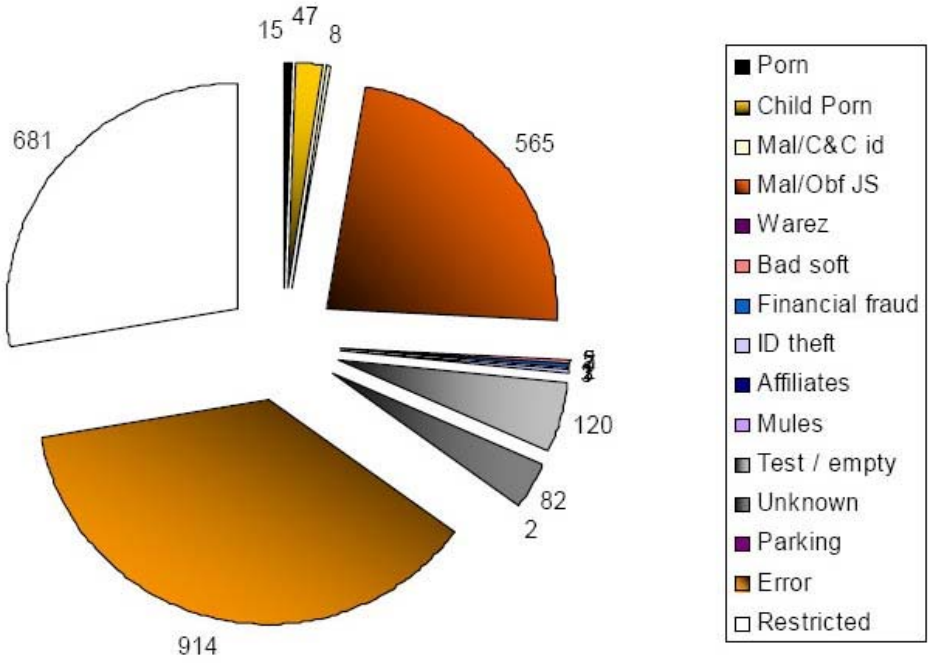
- Distribution of *malware*: a large amount of malicious code has been distributed through RBN IP addresses (CoolWebSearch, VML exploit, MPack, Torpig/Sinowal, Haxdoor, Pinch, Storm and many more);

- *Phishing*: RBN servers hosted a large number of *Trojan horses* programmed to attack e-banking systems. Numerous leads concerning attacks against Swiss banks could be traced to the RBN infrastructure;

[41] Russian Business Network study, David Bizeul: http://bizeul.org/files/RBN_study.pdf (as of: 21.02.2008).

- Other criminal activities, such as hosting Rustock – malware used to send "stock pump and dump spam"[42] – or launching DDoS attacks against financial institutions. RBN has also been identified by Spamhaus.org as a provider for a large number of illegal activities.

In his analysis, David Bizuel finds that the IP address block owned by RBN encompasses 406 activated addresses. These 406 servers hosted 2,090 domain names. The activities of these websites are summarized in the following chart:



RBN is a very complex system. It is affiliated with numerous other companies whose sole purpose is to hide the command centre better and especially to enable RBN to associate itself with other, legal providers and to avoid isolation. Companies such as Nevacom, RusTelekom, AkiMon, Silvernet, Datapoint, Infobox and SBT-Telecom are closely connected with RBN. Searching through the data in the directories of the providers or directories stored elsewhere, one finds that the same persons are responsible for several URLs/DNS. Often mentioned in this connection is Vladimir Kuznetsov[43], who is considered the leader of the RockPhish Group. This is an organization suspected of authoring numerous phishing scams.[44]

But RBN, which is becoming increasingly known even outside the specialized press[45] and is often mentioned in forums and blogs[46], decided in November 2007 to step out of the limelight. One of the first changes noticed was the fact that all domain names containing

---

[42] For further information, see MELANI semi-annual report 2007/I: http://www.melani.admin.ch/dokumentation/00123/00124/01029/index.html?lang=en (as of: 21.02.2008).
[43] http://labs.idefense.com/presentations/online/replays/rbn_2007_08_08.php (as of: 15.02.2008).
[44] For more information on the RockPhish Group, see MELANI semi-annual report 2006/II: http://www.melani.admin.ch/dokumentation/00123/00124/01019/index.html?lang=en (as of: 15.02.2008).
[45] http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461.html (as of: 15.02.2008).
[46] E.g.: http://rbnexploit.blogspot.com (as of: 21.02.2008).

malware suddenly switched to a provider in the Czech Republic (UPL Telecom). RBN then bought eight Chinese IP address blocks, which were blocked several days later, however[47].

Several sources suspect that RBN is looking for a new strategy to survive better. Being a major provider entails undesired visibility. Breaking up into many small and easier-to-hide units is perhaps the best method, even though more resources have to be invested. Another option could be the use of *botnets*[48].

5.4 Terrorism

"Cyber Jihad" (DDoS Attack) Announced for 11 November 2007 Fails to Materialize

At the beginning of November, the Israeli website DEBKAfile warned of an alleged "cyber jihad" planned by al-Qaeda for 11 November 2007.[49] The attacks failed to materialize. Already in previous years, warnings were circulated of alleged imminent terrorist web attacks that did not come to pass.[50] In this case as well, the possibility of a large-scale web attack by terrorists, as well as the seriousness of the report, were met with scepticism by experts from the outset.[51]

According to this warning, a *DDoS attack* was to be launched on that day, shutting down Western, Jewish, Israeli, anti-Muslim, and Shi'ite websites. The attack was initially supposed to affect 15 websites, spreading step-by-step to others.[52]

According to experts, such an attack could be carried out using the "Electronic Program of Jihad" software. Using this software, the attack would not be launched from a botnet consisting of compromised computers, but rather by many different computer users downloading this software individually.[53] The result would thus be a manual botnet, the success of which would depend on coordination among a very large number of participants.

This example shows once again that cyberterrorism – i.e. an attack on the Internet or *critical national infrastructures* by means of IT – still represents only a minor threat even today. In principle, terrorist organizations appear to want to cause as much fear and terror as possible with their actions, for which physical attacks are more suited. Additionally, terrorists rely primarily on the Internet for purposes of propaganda, ideologization, communication, and obtaining information and funding. It is very unlikely that terrorist groups already have the necessary know-how for an attack on critical infrastructures using information technology. As far as politically motivated attacks against individual websites are concerned, they are

[47] http://theregister.co.uk/2007/11/13/rbn_quits_china/ (as of: 15.02.2008).
[48] http://rbnexploit.blogspot.com/2008/01/rbn-out-with-new-and-in-with-old.html (as of: 15.02.2008).
[49] http://www.debka.com/headline.php?hid=4723 (as of: 13.02.2008).
[50] For instance, the U.S. Department of Homeland Security (DHS) warned the financial world at the end of 2006 of a potential attack by al-Qaeda on banking systems. The attack did not occur.
[51] See, e.g., http://dshield.org/diary.html?storyid=3615 (as of: 13.02.2008).
[52] http://www.debka.com/headline.php?hid=4723 (as of: 13.02.2008).
[53] For information on software, see: http://www.darkreading.com/document.asp?doc_id=128281; http://www.theregister.co.uk/2007/11/08/electronic_program_of_jihad_discovered/ and http://www.networkworld.com/news/2007/103107-report-cyber-jihad-set-for.html?nlhtsec=1029securityalert4&&nladname=110107securityal (as of: 13.02.2008).

nothing new and also have a limited impact. The DDoS attack against Estonia at the beginning of 2007 was new in terms of its scope, however.[54] A massive DDoS attack by terrorists, as was supposed to happen in this case, is unlikely, however, in the view of MELANI. A much greater threat against Internet security and the infrastructures depending on it continues to emanate from Internet crime in general. As the next section show, terrorist organizations also use methods of Internet crime to obtain financing.

Suspected Connection Between Terrorism and Internet Crime Confirmed

In July 2007, Younis Tsouli, known as "Irhabi007", was sentenced to ten years in prison for incitement to murder. This case shows to what extent terrorists use the Internet for purposes of propaganda, radicalization, communication, and obtaining financial resources, but also how the Internet links up with terrorism in the real world. In particular, this case confirms the link between terrorism and Internet crime, and that terrorists are using the Internet to obtain financial resources.[55]

With credit card access data obtained via *phishing* attacks and the distribution of Trojans, Tsouli and his two co-conspirators obtained the financial means to fund the recruitment and support of potential jihadists. 37,000 stolen credit card numbers and the associated personal data were found on one of their computers. These stolen data were used to purchase equipment and material (airline tickets, prepaid phones, etc.) and to register websites. These websites hosted content such as instructions on how to build bombs and hack computers, as well as videos of attacks.[56]

The Internet allows people – far removed from terrorism in the real world – to play a significant role in the areas of ideologization, recruitment, communication, and financing of international terrorism. This case confirms in particular that terrorists use Internet crime to obtain financial resources. Not only individual criminals and organized crime, but also terrorists have thus discovered Internet crime as a source of funds.

[54] On the DDoS attack against Estonia, see Chapter 5.1 of the MELANI semi-annual report 2007/I: http://www.melani.admin.ch/dokumentation/00123/00124/01029/index.html?lang=en (as of: 21.02.2008).
[55] For more information on this case, see: http://news.bbc.co.uk/1/hi/uk/6273732.stm; http://www.economist.com/world/displaystory.cfm?story_id=9472498; http://www.washingtonpost.com/wp-dyn/content/article/2007/07/05/AR2007070501153.html; http://counterterrorismblog.org/2008/01/credit_cards_and_terrorists.php and http://www.spiegel.de/politik/ausland/0,1518,495468,00.html (as of: 13.02.2008).
[56] See: http://www.washingtonpost.com/wp-dyn/content/article/2007/07/05/AR2007070501945_pf.html (as of: 13.02.2008).

6 Prevention: Protection Of Computers And Servers

Both in the private and the corporate realm, the human/computer interface has moved further into the focus of attackers. Of primary interest are data that can be converted into money. But also computer performance and bandwidth can be stolen and sold with profit to *spammers*, *phishers*, or *DDoS attackers*. Attackers are therefore interested in every single computer.

The two last semi-annual reports focused on the topics of *social engineering* and *drive-by protection.* In this chapter, we will focus on measures to support prudent users. In addition to website visitors (6.1), we will also address our remarks to web administrators (6.2). Using simple methods, the goal is to reduce the probability of becoming infected by malware.

A project conducted in May 2007 analyzed 4.5 million websites for the presence of *malware* and determined that 10% were clearly infected, and a further 700,000 websites triggered the download of suspicious programs. Moreover, the study found that malware also appears in areas where website operators do not feel responsible, such as *banner* advertisements.[57] The risk of unintentionally having malware uploaded to one's own website not only affects private hobby administrators, however. In February 2007, the website of the Miami Dolphins, an American football team, was hacked shortly before the Super Bowl and infected with malware, which in turn attempted to infect the computers of visitors.[58]

Especially in connection with the Euro 08 football championships, official and private websites are being set up in Switzerland that could easily become a focus of such drive-by infections.

6.1 From The User Perspective

Risks

A careful approach to e-mails and downloaded software should go without saying nowadays. Automatic updates of the operating system and browser, anti-virus software, and firewall are also part of the basic protection of every computer.[59] When selecting a firewall, you should ensure that the firewall is able to monitor both incoming and outgoing traffic, and that it notifies you if, for instance, a new program wants to access the Internet. A list of links to firewall software is available on the MELANI website[60]. But even if you abide by the usual rules of conduct, there is no 100% protection against damage nowadays. An increasingly important reason for this is *drive-by infections*. Infections with *malware* can occur even if a website is simply visited.

---

[57] See: http://www.pcwelt.de/start/software_os/sicherheit/news/80130/ and http://www.usenix.org/events/hotbots07/tech/full_papers/provos/provos.pdf (as of: 13.02.2008).

[58] For more information, see: http://blogs.zdnet.com/security/?p=15 and http://www.sophos.com/pressoffice/news/articles/2007/02/superbowl.html (as of: 13.02.2008).

[59] Rules of conduct available at: http://www.melani.admin.ch/themen/00166/00172/index.html?lang=en (as of: 14.02.2008).

[60] http://www.melani.admin.ch/dokumentation/00126/index.html?lang=en#sprungmarke0_5 (as of: 14.02.2008)

Although technical measures cannot completely eliminate the probability of an infection, they can nevertheless reduce it. As a general remark, it should be noted that such measures may entail extra work and, in most cases, also reduce user-friendliness. In light of the existing dangers, however, the additional effort is reasonable and certainly less than would be necessary to remedy damage after it has occurred.

Prevention

- **Surfing with a restricted account or in a sandbox**

  One widespread bad habit is the negligent use of accounts with administrator privileges. Such privileges are, for instance, the default option in many Microsoft Windows operating systems. When surfing the Internet, the use of a restricted account can improve security. This security measure is especially useful with respect to *drive-by infections*, since the user is asked to enter the administrator password before installing (unwanted) programs. But this measure also helps when clicking on programs that are concealed as unsuspicious documents. If the user enters the administrator password without thinking every time it is requested, however, this measure is of course useless.

  The simplest way to protect oneself against drive-by infections is to set up a separate work account with restricted privileges. Administrator privileges should only be used when intentional system modifications are carried out. A restricted account also offers the possibility of restricting browser privileges, as the following section shows. In addition, there are already programs and functionalities that allow the browser to operate in a "protected" zone. Since most surfers use Internet Explorer, this is the biggest target for malware authors. For other browsers such as Mozilla Firefox and Opera, there are fewer known *exploits*.

- **Surfing without ActiveX and JavaScript**

  While some websites only consist of text documents and do not offer any additional functions, other sites also exhibit dynamic content. Examples are tickers, web forms for online orders, animated images, and dynamically displayed advertising banners. Such dynamic functions may be implemented with ActiveX controls and JavaScript. Surfing without these functions activated is admittedly tedious, but it increases security considerably, since drive-by infections still predominantly exploit ActiveX. For this reason, the security settings on Internet Explorer should be set to "high". Since Active Scripting is used on may websites on the Internet, some websites can no longer be displayed to the full extent using the "high" security setting. For this reason, we recommend including individual websites (that you trust) in the list of "trusted sites". The method is described in the document "Security settings for Windows XP".[61] For Firefox, the NoScript plug-in[62] can be used, where JavaScript is prohibited in general and individual (trustworthy) sites can also be activated. A description is contained in Annex 10.2.

- **Update of add-ons (plug-ins) and applications**

  It is not only important to keep browsers and operating systems updated; the same also applies to plug-ins and applications. *Vulnerabilities* in popular applications such as Flash

[61] http://www.melani.admin.ch/dienstleistungen/00133/00157/index.html?lang=en and http://www.melani.admin.ch/dienstleistungen/00132/00149/index.html?lang=en (as of: 14.02.2008)
[62] https://addons.mozilla.org/de/firefox/addon/722 (as of: 14.02.2008).

Player, RealPlayer, WinZip and many other programs are increasingly being targeted by attackers. It is therefore important to have an overview of the add-ons and applications installed on the computer. Browser plug-ins may, for instance, be viewed under Tools ➔ Add-ons or "Manage add-ons". Both Firefox and Internet Explorer have an add-on update function. Wherever available, an automatic update function should be used. Detailed instructions for Internet Explorer are contained in Annex 10.2. The list of installed software in Windows can be accessed with Start ➔ Control Panels ➔ System ➔ Software.

Programs monitoring the update status of programs (such as Secunia Software Inspector[63]) may help maintain an overview of whether installed programs are up-to-date.

6.2 From The Website Operator Perspective

Risks

With the increasing use of the Internet for information exchange and the increasing availability of administration programs for websites, the number of private persons who set up complex websites is also growing. With "Web 2.0" or content management systems (CMSs), there are many options for producing simple multimedia websites for free with interactive content (blogs, forums, wikis, etc.). Software packages for this purpose, such as Joomla, are complex, however, and rely on several different building blocks. Each building block, but also the operating system underlying it, may contain vulnerabilities, which must then always be updated where possible. In addition, there are unknown vulnerabilities, used by so-called *zero-day exploits.*

Many users are not aware of this complexity, but rather are excited by the simplified possibilities for building expanded functions into websites. If these programs are poorly maintained, however, they may constitute an attractive target for perpetrators to distribute malware. Many operators of websites are not professional IT specialists. Websites operated by professionals are also not immune to poor maintenance: Even professionals are not always sensitized sufficiently with respect to security.

Interactive user elements employed in forums or wikis offer another point of attack. Poor control of user-typed entry fields and poorly-configured default settings in forum software or forms may, in the worst case, allow attackers to access the server and/or data. Full access then allows pages or inconspicuous page elements (such as the banner advertisements mentioned above) to be set up containing *drive-by infections.*

Passwords that are easy to guess, installed *keyloggers*, or hacked (home) computers may also allow access to administrator consoles or web interfaces.

[63] http://secunia.com/software_inspector/ (as of: 14.02.2008).

Prevention

Operators of websites can protect both the site and its visitors from malware by observing three principles:

- Website administrators should know the web software they use as well as the versions of the operating systems, and pay attention to their configurations.
- Automatic updates of web server operating systems and a regular search for application updates. These updates can be partially automated with Windows and Unix systems. Operators should regularly obtain information on potential vulnerabilities and updates of the programs they use.
- Occasional scanning (active inspection) of one's own website for malware, using general IT security tools such as Nmap, Nessus, etc., especially after installing new functions.[64] IT security export Niels Provos has developed a program named SpyBye[65], which allows webmasters to scan their sites for malware.

7 Activities / Information

7.1 State

Germany: Entry into Force of the Law on the Retention of Data

The new law governing telecommunication surveillance has been in force in Germany since 1 January 2008[66], thus implementing the EU directive on the retention of data into German law.[67] Telephone and Internet communications must be stored for six months without the need for a concrete suspicion. Internet providers have been granted a transition period until January 2009 to comply. The new law is heavily contested, and a constitutional complaint has been submitted to the Federal Constitutional Court of Germany.[68]

---

[64] See: http://nmap.org und http://www.nessus.org/nessus/ (as of: 13.02.2008).

[65] The program is described in the book "Virtual Honeypots: From Botnet Tracking to Intrusion Detection“ (Provos and Holz, Addison-Wesley 2007) pp. 268 et seqq. See also: http://monkey.org/~provos/spybye/ and http://www.spybye.org (as of: 13.02.2008).

[66] For the text of the law, see: http://www.bundesrat.de/cln_051/SharedDocs/Drucksachen/2007/0701-800/798-07,templateId=raw,property=publicationFile.pdf/798-07.pdf (as of: 13.02.2008).

[67] For the EU directive, see: http://www.bmj.de/files/8bb57015feb3792008793d7535469da9/2552/EU-Richtlinie%20Vorratsdatenspeicherung.pdf (as of: 13.02.2008).

[68] On the constitutional complaint, see: http://www.heise.de/newsticker/meldung/100737; http://www.vorratsdatenspeicherung.de/content/view/184/79/; http://www.heise.de/newsticker/meldung/101073 and http://www.heise.de/newsticker/meldung/101159 (as of: 13.02.2008).

Switzerland already regulates the retention of data. Under the Federal Law on the Surveillance of Mail and Telecommunications, telecommunication service providers must retain certain communication data for a period of six months.[69]

ITU: Creation of a High Level Expert Group

On 17 May 2007, the International Telecommunication Union (ITU) published its two-year Global Cybersecurity Agenda. The Agenda considers international and intersectoral coordination and the creation of international standards and laws indispensable. It justifies this demand with reference to the increasingly networked nature of society, industry, and States, and their growing dependence on information and communication technologies. Only in this way can threats and weaknesses be successfully contained and combated. The ITU, with its 191 member States and 700 partners from a wide range of private sector industries and non-governmental organizations, considers itself in the best position to advance the elaboration of such comprehensive and multilateral concepts. The focus should be placed on the following topics in particular: the development of the legal framework, and the establishment of institutions and binding standards in the field of ICT resources, with a view to combating the increase in computer crime.

Against this backdrop, the ITU has now established a High Level Expert Group (HLEG), which met for the first time on 5 October 2007. It is composed of about 60 experts from government and administration, industry, international organizations, and research. The goal of this group is to prepare strategy papers for the Chairman of the ITU in the fields of legal, technical, and procedural measures, international cooperation, the establishment of competences, and the development of organizational structures. First drafts of these papers have been available since February 2008.

With the publication of its Global Cybersecurity Agenda (GCA) in May 2007, the ITU has set the bar high: By 2009, it aims to achieve a global legal, organizational, and technical approach adopted by the majority of countries, to combat the threats in the field of information and communication technology, including the Internet. The task of the HLEG encompasses not only the elaboration of new concepts in the sectors described, but also reconciliation of these concepts with the existing international conventions, standards, and requirements, e.g. with the already existing ISO standards relating to ICT security or the Cybercrime Convention of the Council of Europe, which provides for international harmonization of the various criminal legal foundations and a rapid, abbreviated legal assistance procedure between signatory States. Accordingly, the goal of the individual States represented in the HLEG is not to reinvent the wheel, but especially to play a coordinating and subsidiary role. Switzerland is represented in the HLEG by staff members of the Federal Office of Communications and of the Reporting and Analysis Centre for Information Assurance (MELANI).

The GCA also offers the ITU the possibility of re-establishing a leadership position with respect to the Internet, namely in the field of ICT security and more efficient international cooperation to combat threats to the information society.

[69] BÜPF, SR 780.1: http://www.admin.ch/ch/d/sr/7/780.1.de.pdf (as of: 13.02.2008).

Germany: Entry into Force of A Hacker Article

In August 2007, an amendment of the German Criminal Code entered into force, the so-called "hacker article". This article criminalizes preparations for the criminal act of spying out or intercepting data by manufacturing, procuring, selling, transferring, disseminating, or granting access to passwords, other security codes for data access, as well as computer programs for these purposes.[70]

Critics fear that this article also criminalizes software used by IT experts to analyze vulnerabilities. MELANI views it in principle as a positive development to punish the dissemination and manufacture of malicious software with a clear criminal background. However, a blanket criminalization of software also used to test the vulnerability and security of IT systems in the first place would be problematic. Future jurisprudence will show how the law is implemented in practice.

United Kingdom: Entry into Force of Part III of the Regulation of Investigatory Power Act

In October 2007, Part III of the Regulation of Investigatory Power Act entered into force in the UK. The Regulation of Investigatory Power Act was enacted in 2000 to provide law enforcement authorities with additional investigation and surveillance options in an era of advancing computer technology. Part III now allows law enforcement authorities to demand the disclosure of passwords and crypto keys under the threat of imprisonment. The law aims to make it more difficult for criminals and terrorists to hide their data by means of encryption.[71]

Criticism of this law focuses on several points. Opponents fear that a disclosure requirement for keys may chase financial sector companies in particular out of the country. The requirement to disclose keys may endanger the confidentiality of all data encrypted with such keys. Moreover, the effectiveness and implementation of the law are being called into question, since suspects may simply claim that they have lost or forgotten the keys. In addition, many encryption products use so-called *containers*. Even if the outermost container is decrypted, the mere existence of a hidden internal container may be disputed.[72]

In Switzerland, no provisions exist that allow law enforcement authorities to enforce the disclosure of passwords with the threat of several years of imprisonment. It is a principle of Swiss criminal procedure that no one may be required to incriminate himself or herself. This principle is also enshrined in international law, including the International Covenant on Civil and Political Rights.

---

[70] For § 202c of the Criminal Code, see: http://www.gesetze-im-internet.de/stgb/__202c.html and for the penal provisions to combat computer crime: http://www.bgblportal.de/BGBL/bgbl1f/bgbl107s1786.pdf, for additional information on the topic, see: http://www.heise.de/newsticker/meldung/94190 (as of: 13.02.2008).

[71] RIPA 2000: http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1, for more information on Part III of the Act, see: http://security.homeoffice.gov.uk/ripa/encryption/ (as of: 13.02.2008).

[72] See: http://news.zdnet.co.uk/security/0,1000000189,39289786,00.htm,; http://news.zdnet.co.uk/security/0,1000000189,39269746,00.htm and http://www.heise.de/newsticker/meldung/97050 (as of: 13.02.2008).

7.2 Private sector

Improved Security Measures for E-Banking

Various financial institutions are currently testing or introducing new authentication methods. All of these methods attempt to achieve security gains while maintaining user-friendliness to the extent possible. The most popular methods are the transmission of transaction data via a second channel (mobile telephone) or a hardened browser given to clients on a USB stick, for instance. Another method is transaction authorization by cryptographic calculation of the transaction number (TAN).[73] Unlike transaction authorization with a simple TAN, the TAN here is directly connected to the transaction being authorized. Parameters for the calculation include transaction data, such as the account number of the recipient or the amount transferred. The calculation is carried out on an external reader with a cryptographic processor.

The "Internetpassport" smart card developed by a Swiss company also permits the cryptographic calculation of TANs. Transaction data need not be entered by hand, but are transferred to the card using optical signals (via the computer display). The client must then verify the transaction data on the display of the card and is given a code to be entered on the computer for confirmation.[74]

Transactions that must be verified and confirmed via a second authentication channel, as well as authorization by cryptographic calculation of the TAN, are currently considered secure. The user tends not to notice manipulations, however, since he or she pays too little attention to the message indicated on the display. Recipient numbers entered by hand require more effort, but they protect the user from his or her own negligence.[75]

No uniform e-banking authentication method appears to be emerging in Switzerland. However, the trend from session authentication toward transaction signature is likely to continue.

8 Legal Foundations

Single Euro Payments Area Planned

A Single Euro Payments Area (SEPA) is planned throughout Europe, which will allow faster and cheaper cross-border payments in the future. The legal basis is given by the EU Payment Services Directive, which must be implemented into national law by 1 November 2009. The starting date of SEPA was 28 January 2008. The SEPA procedure will now replace the existing national procedures for euro payments step-by-step. In particular, cross-

[73] http://www.bw-bank.de/privatkunden/1000006911-de.html (as of: 13.02.2008).

[74] http://www.axsionics.ch/tce/frame/main/471.htm (as of: 13.02.2008).

[75] See "Aktuelle Malware-Angriffe gegen Online-Banking-Portale: Lösungsansätze für sichere Authentifizierung und Zahlungsabwicklung", diploma thesis at the Lucerne University of Applied Sciences, T. Holderegger, 2008.

border transfers must be as rapid and cheap as national transfers by 2012. Instead of the three to five working days now usual, payments abroad should then be concluded by the end of the following working day. Switzerland is also participating in SEPA, but is not bound by the EU directive.[76]

For an assessment of the impact of SEPA on the recruitment of "money mules" and money laundering, see Chapter 3.2.

[76] For the Payment Services Directive, see: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:319:0001:01:EN:PDF, for additional information, see also http://www.sic.ch/tkicch_home/tkicch_standardization/tkicch_standardization_sepa.htm (as of: 13.02.2008).

9 Glossary

This glossary contains all the expressions in *italics.* A more extensive glossary containing even more expressions can be found at:
http://www.melani.admin.ch/glossar/index.html?lang=en.

Banner	Element of a webpage that displays advertisements. Banner elements can serve as inconspicuous vectors for attacking websites, since the content is rarely verified by the web administrators.
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.
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
Bulletproof hosting	"Bulletproof" provision of services or storage space without the usual content restrictions. This content can include hard (child) pornography, phishing sites, and other illegal content. The operators protect their clients from competitors' attacks and do not cooperate with law enforcement authorities. The Russian Business Network (RBN) is known for such bulletproof hosting services.
Click fraud	Click fraud is a type of Internet fraud that primarily targets banner advertisements paid per click. Click fraudsters may operate manually or with the help of programs. These programs simulate banner clicks to manipulate the underlying accounting systems.
Client	Programs or computers that access information through a direct connection with a server.
Container	A file containing an encrypted file system. When a password is entered, the container appears transparently as a normal drive to the user. When the user logs off, the container is closed, and the data are only available in encrypted form.
Critical (national) infrastructure	Infrastructure or part of the economy whose failure or breakdown would have enormous consequences on national security or the economic and/or social welfare of a nation. In Switzerland the following infrastructure has been defined as critical: energy and water supply, emergency and rescue services, telecommunications, transport and traffic, banks and insurance, government and public administration. In the information age their smooth running is increasingly dependent upon information and communication systems. Systems such as these are referred to as critical information infrastructures.

Crypter	Encryption tool, encryption algorithm. (Part of a program responsible for encryption).
DDoS attacks	Distributed denial of service attacks A *DoS attack* where the victim is simultaneously attacked by many different systems.
DNS	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.
Downloader	Initial component of a malware infection, may lead to an infection with further malicious programs. The downloader downloads the actual virus, Trojan, etc., and launches it on the infected system.
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.
Exploit code	(or exploit) A program, a script or a line of code with which vulnerabilities in a computer system can be used to advantage.
IP address	Address to uniquely identify computers on the Internet or on a TCP/IP-network (e.g.: 172.16.54.87).
Keylogger	Devices or programmes in operation between the computer and the keyboard to record keystrokes.
Malware/Malicious Code	Comes from the terms "malicious" and "software". Generic term for software which carries out harmful functions on a computer. This comprises amongst others viruses, worms, Trojan horses. See also Malware.
Packer	Compression program or compression algorithm of a program. Originally intended to optimize the size of a program on the hard drive. Malware often uses upstream packers to prevent recognition by anti-virus software and to make analysis of the malware (reverse engineering) more difficult.
Patch	Software which replaces the faulty part of a programme with a fault-free version. Patches are used to eliminate security holes (*vulnerabilities)*.

Phishing	Fraudsters phish in order to gain confidential data from unsuspecting Internet users. This may, for example, be account information from online auctioneers (e.g. eBay) or access data for Internet banking. The fraudsters take advantage of their victim's good faith and helpfulness by sending them e-mails with false sender addresses.
Plugin	(Additional) software that extends the basic functions of an application, e.g. Acrobat plugins for internet browsers allow direct display of PDF documents.
P2P (Peer to Peer)	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.
Ransomware	A form of malware used to extort money from the owners of infected computers. Typically, the perpetrator encrypts or deletes data on an infected computer and provides the code needed to recuperate the data only after a ransom has been paid.
Relay	A relay is a system acting as an interim station for the provision of a service. In connection with malware and spam, relays are used to conceal the real sender and prevent blocking. Open SMTP relays are of particular note. These are computers that accept e-mails from any given computer and forward them to third parties, even though they are not responsible for the e-mails of either party. Botnets are often also used for relay purposes. Internet Relay Chat (IRC) is also significant in this connection, since it is often abused as a communication interface for botnets.
Rootkit	A rootkit is a collection of software tools that are installed on a compromised system once it has been penetrated, in order to conceal the presence of the intruder (hacker or *malware*) and hide processes and files. Rootkits are important components of malware, for instance to prevent the malware from being identified by anti-virus programs.
Social Engeneering	Social engineering attacks take advantage of people's helpfulness, credulity or lack of self confidence in order to gain access to confidential data or to prompt them to perform certain actions, for example.
Spam	Spam refers to unsolicited and automatically sent mass advertis-ing, into which category spam e-mails also fall. The person re-sponsible for these messages is known as a spammer, whereas the actual sending itself is known as spamming.
Squatter	Squatters are persons or organizations who register Internet domains with slight typographic modifications, in the hope that users will mistype and accidentally land on these websites (e.g.: www.melani.admim.ch instead of www.melani.admin.ch). This can be used to place advertisements on these sites, but also to distribute malware. The term is also applied to persons who register unused, attractive domains in the hope of reselling them later on.
Supernodes	In *peer-to-peer networks*, supernodes are responsible for data flow and the connections with other users; they serve as *relays* and

	proxies.
Trojan horses	Trojan horses (often referred to as Trojans) are programs that covertly perform harmful actions while disguised as a useful application or file.
Vulnerability	A loophole or bug in hardware or software through which attackers can access a system.

10 Appendix

10.1 Botnets with Fast Flux

Botnets: Survival Thanks to New Developments

Like every legal economic activity, illegal conduct on the Internet primarily pursues the fundamental goal of ensuring its own survival. In the world of computer crime, one must hide to survive; one must trick investigators into following the wrong clues, and one must cover one's tracks. IRC *botnets*[77] – computer networks infected with *malware* and receiving commands from a central IRC server to carry out various tasks (*spam*, *DDoS attacks*, *bulletproof hosting*, etc.) – have a vulnerable architecture. If the central IRC server is discovered, the entire network can be deactivated.
To improve the resistance of these networks, new techniques have been developed: Decentralized (serverless) systems have been surfacing, based on *peer-to-peer* protocols (the same development as in other areas, such as online music sharing, from Napster to Kademlia). Botnets are also beginning to rely on so-called fast-flux service networks. In this Annex, we discuss these new trends in detail, which mark an important evolutionary step in the field of computer crime.

Further Development of Command and Control: P2P

The term "command and control" (C2) refers to the command centre of a botnet. The most popular method so far has been the use of Internet Relay Chat (IRC) as the neuralgic point of the system architecture (see Figure 1). To guarantee a longer life for the IRC server and hence for the botnet, various techniques are employed: e.g. the encryption of messages between the client IRC and the server, or the frequent shifting of servers. But this is not enough to ensure the survival of the server. Computer criminals are always trying to harden their infrastructure; the current goal is therefore to eliminate dependency on a central server.

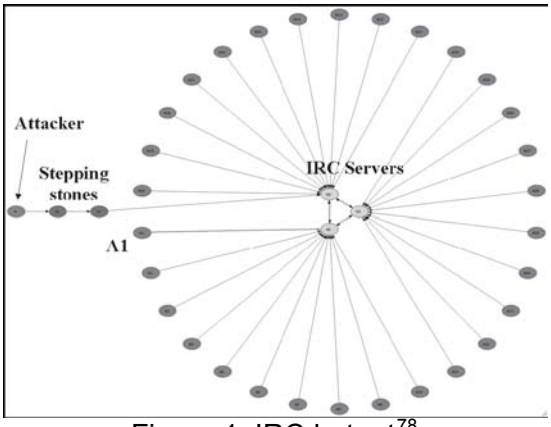


Figure 1: IRC botnet[78]

[77] For more information, see MELANI semi-annual report 2005/II: http://www.melani.admin.ch/dokumentation/00123/00124/00161/index.html?lang=en (as of: 21.02.2008).
[78] Source: "Command and control structures in malware: from handler/agent to P2P", LOGIN: Vol.32, No.6, http://www.usenix.org (as of: 14.02.2008).

This consideration gave rise to the use of decentralized P2P networks for online music sharing. The first version of music sharing via a P2P system was Napster (1998). In brief, a user logged on to the Napster server to obtain the IP address of other users making the desired song available. As soon as this information was received, the users linked up directly so that both could access the sound file. The further development of these systems led, for instance, to Kademlia[79], a network used by the well-known P2P systems such as Overnet (Overnet, MLDonkey), Kad (eMule, aMule, MlDonkey), BitTorrent (the original BitTorrent, but also Azureus, BitComet, µTorrent). Simply put, Kademlia uses a distributed ID table or list called a distributed hash table (DHT) that creates a network in which each node (client) is labelled with an ID number. Each node contains the information necessary to receive a file or service – no server is needed. Criminals have adopted P2P techniques and given life to a new bot generation (see Figure 2).

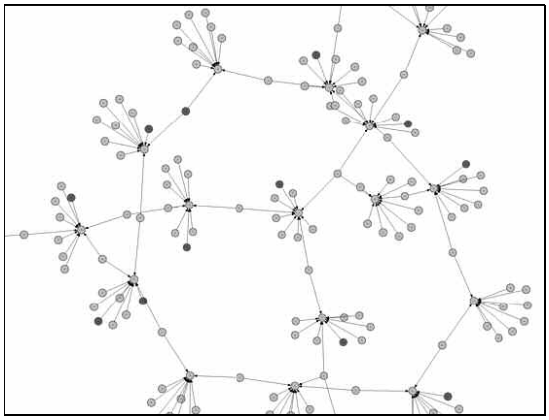


Figure 2: Possible structure of a botnet based on P2P[80]

One of the best-known botnets, Storm (see also Chapter 5.2) uses the Overnet protocol for the distribution of information and for the delivery of the desired functions to the infected peers. According to an analysis of Storm[81], every newly infected computer contains a list with 300 peers indicating the hash function, IP address, port, and peer type. Using this list, the new network member can log in and obtain the most recent information on the network status. Very high-performance peers (with respect to uptime and connection speed) become servers storing e-mail templates, e-mail lists, and mail servers (Storm is primarily a bot for the dissemination of spam). The information is not sent by the server as such, but rather each botnet member picks it up. Compared with other developments, such as fast flux (see below), P2P botnets practically never use *DNS* services. Since DNS is not used for the distribution of peer lists, the identification of a C2 channel, or logging on to the network, DNS-based identification techniques are ineffective against this type of structure. Storm only uses DNS for MX (mail exchange record) lookups. If Storm were used for DDoS attacks, such DNS lookups would certainly be carried out.

It is not easy to trace such bots in the network. Distinguishing legitimate P2P traffic from Storm-based traffic is a very difficult challenge. It would be much easier to simply monitor TCP/25 ports for a higher level of activity. But this would be a reactive measure on a very specific computer. Moreover, malware such as Nugache and Storm add in a rootkit to make tracing more difficult.

---

[79] http://pdos-csail.mit.edu/~petar/papers/maymounkov-kademlia-lncs.pdf (as of: 13.02.2008).

[80] Source: “Command and control structures in malware: from handler/agent to P2P”, Dave Dittrich, Sven Dietrich, LOGIN: Vol.32, No.6, http://www.usenix.org (as of: 14.02.2008).

[81] “Analysis of the Storm and Nugache trojans: P2P is here”, Sam Stover, Dave Dittrich, John Hernandez, Sven Dietrich, LOGIN: Vol.32, No.6, http://usenix.org (as of: 14.02.2008).

Storm and Nugache are the first examples of the use of P2P technology for botnets. Criminal groups are currently trying to avoid using central servers – the weakest links – and to move to decentralized networks: As soon as these new systems have matured, they will serve as the basis for most criminal Internet activities.

Fast Flux

Botnet operators are increasingly employing fast-flux[82] techniques in order to enhance the reliability of their networks and to make identification of the networks more difficult. This also enhances the attractiveness of the networks for phishers, for instance.

By using fast-flux functions in botnets, tracks can be covered more easily, and the stability of the system can be ensured more effectively. As in other economic areas, the perpetrators pay attention to cost and security. Security in this context means protection from rivals and law enforcement authorities, and maintaining availability.

When calling up a domain name (www.example.com), for instance in a browser, the *DNS system* translates its name into an *IP address* (192.168.0.1). This IP address in turn is mapped to a server/computer. These mapping tables are stored on a name server. In the case of frequently visited sites such as google.com or admin.ch, several different IP addresses are mapped to a single domain name due to the large number of queries, so that the burden can be distributed among several different computers.

Figure 3: Several IP addresses are mapped to google.com

These mapping tables also give the name-server a time period during which the entry is valid. Once this time period (time-to-live) has expired, the name resolution must be repeated, and new mapping tables may be loaded, which in turn contain new IP addresses and accordingly also refer to different computers. If this procedure is combined with a short time-to-live, it is called fast flux.

Use for Criminals

This technique may now be used by criminals for their own purpose. In this case, the different computers are compromised (*bots)* and contain websites with criminal content. Since these sites constantly change computers, the criminals don't care if a computer is no longer available. Even if some computers are taken out of the network or no longer function, the rest of the network remains. This enhances the stability of the site and makes countermeasures more difficult.

---

[82] As in, "in flux". "Fast" flux refers to the rapid exchange between the individual computers.

A second use is the concealment of an IP address. The final website assignment is constantly changing IP addresses, which protects them from detection. This is shown in Figure 4, where the "zombie home PC" is a member of an entire botnet and is regularly (by minutes or seconds) exchanged with other members. The surfer, e.g. a victim of *phishing fraud* clicking on the link of an e-mail, is now no longer connected directly with a single computer, but rather with a constantly changing botnet member. The phishing site does not necessarily have to be located on this computer, since it suffices to forward the connection to a central server on which the actual data are stored and the control server may be located. This makes command-and-control (C&C) computers (or "motherships") much more difficult to locate. Without this technique, the IP address of the mothership is easily visible.

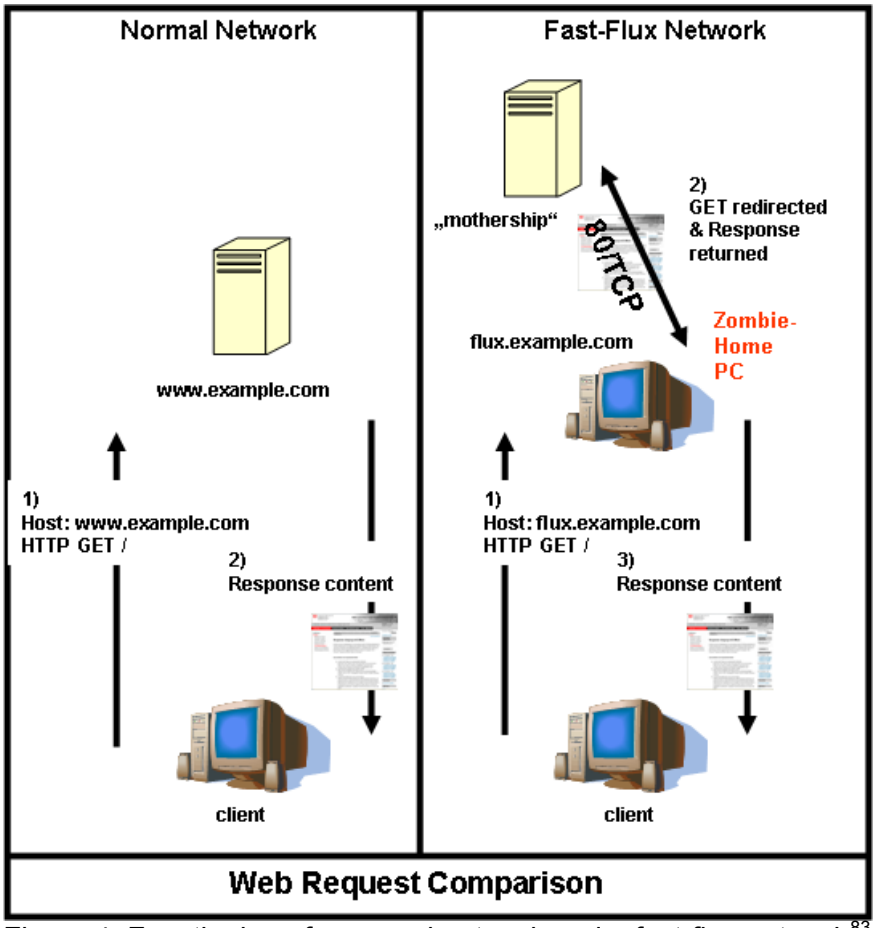


Figure 4: Functioning of a normal network and a fast-flux network[83]

This concealment protects the command-and-control computers, which – unlike the infected botnet members – contain the productive attack codes (the *malware*), the configuration files, or the bogus websites.

Scope of the Problem

In a study by the Honeynet Project[84], researchers observed criminal fast-flux activities for a domain over the course of two weeks in February 2007. This fast-flux network consisted of 3,241 IP addresses, of which 1,516 computers indicated that they were responsible for the domain, and 2,844 of which served as exchangeable interim computers. By July 2007, the

[83] Presented at http://www.honeynet.org/papers/ff/index.html (as of: 14.02.2008).
[84] Presented at http://www.honeynet.org/papers/ff/index.html (as of: 14.02.2008).

researchers observed a total of 80,000 flux IP addresses in more than 1.2 million unique mappings of IP to name. In an update survey, they found 40,000 domains by September 2007, 150,000 flux IP addresses, and 2.5 million unique mappings.[85]

Prevention

When Internet users maintain their home computers appropriately and keep them updated to the most recent security level, this can make the business of botnet operators more difficult. It deprives scammers of the "mass" to hide behind.

In light of fast-flux botnets, ISPs and registrars are also called upon to employ technical means against this Internet plague. Detailed recommendations are contained in the Honeynet document, such as:

- Blocking access to control infrastructure of the criminals.
- Improving domain registrar response procedures to reports of fraudulent domains and new registrations.
- Monitoring and harvesting of DNS datasets.
- *DNS*-based black lists and occasional router changes to block the path to criminal management computers.

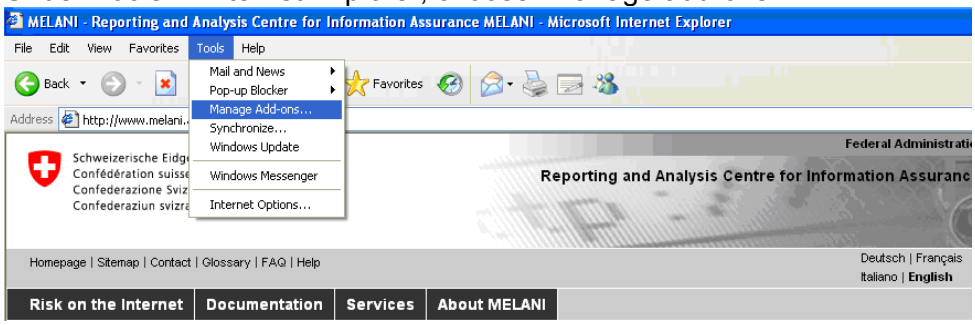
10.2 Technical protection of computers

Management of add-ons

It is important not only to keep browsers and operating systems updated, but also plug-ins and applications. It is important to maintain an overview of the add-ons and applications installed on the computer. This section explains how computer users can tell which plug-ins are installed in their browser, using the two most popular browsers (Internet Explorer and Firefox).

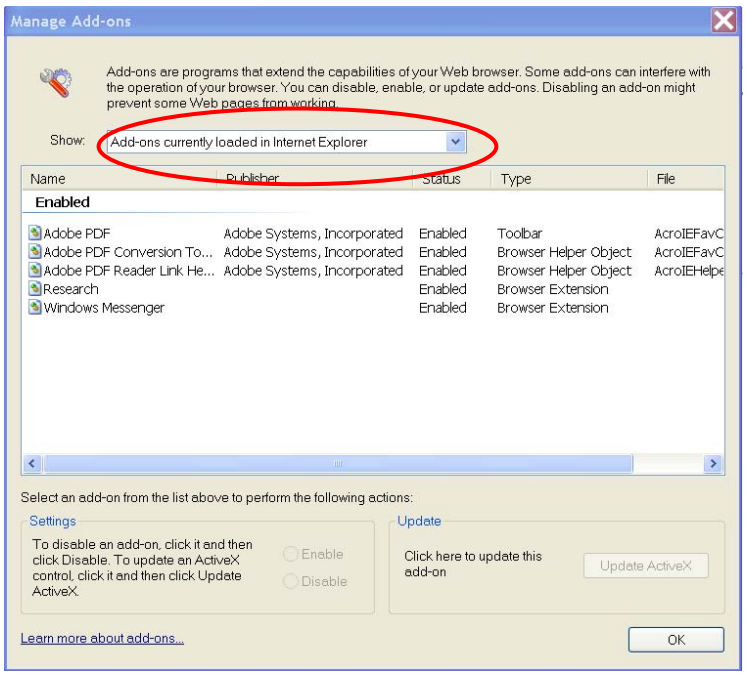
Internet Explorer 6

Under Tools in Internet Explorer, choose "Manage add-ons"...



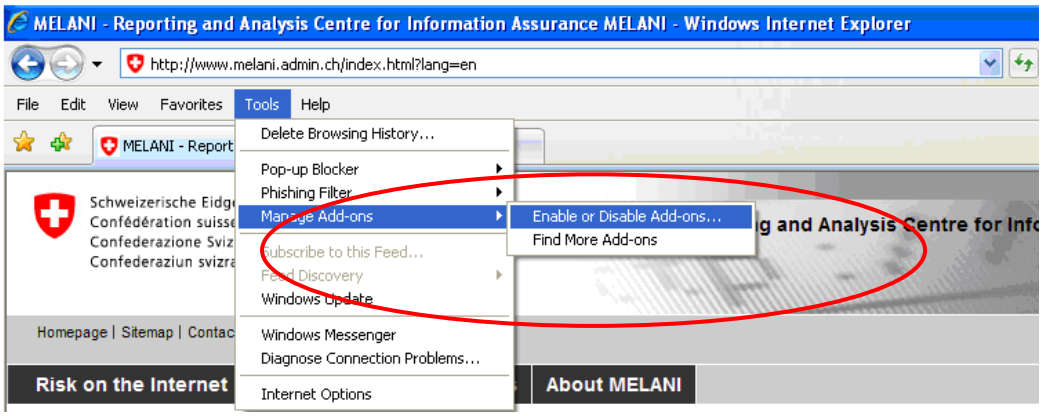
[85] For the update, see Honeynet Project site above, "Fast-Flux PowerPoint Presentation“ (as of: 14.02.2008).

This displays all add-ons loaded in Internet Explorer. You can also display the used add-ons by choosing the appropriate option (circled in red). Add-ons can be activated and deactivated. By clicking on the "Update ActiveX" button, the add-ons can be updated to the most recent version. This function is not possible for all programs.

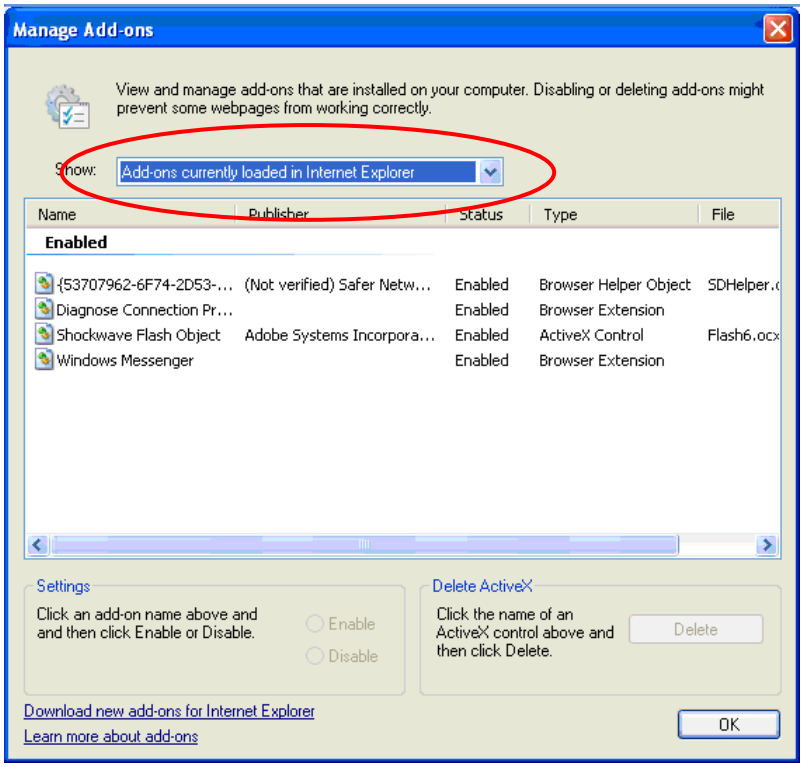


Internet Explorer 7

Under Tools in Internet Explorer, choose "Manage add-ons" and click on "Enable/Disable Add-ons".

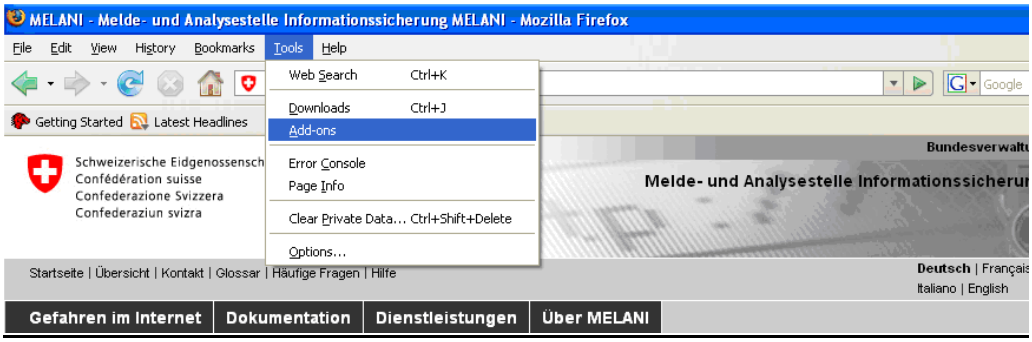


This displays all add-ons used in Internet Explorer. You can also display the loaded add-ons by choosing the appropriate option (circled in red). Add-ons can be activated and deactivated.

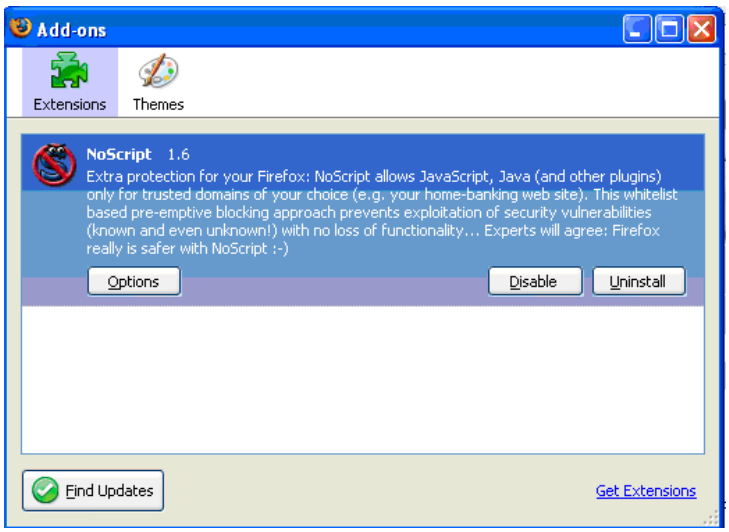


Firefox

Under Tools in Firefox, choose "Add-ons"…



This displays all add-ons used in Firefox. By clicking on "Find Updates", the most recent version of the add-ons can be downloaded. This function is not possible for all programs.



Use of NoScript in Firefox

By installing NoScript, JavaScript content is blocked on almost all sites. Only sites selected by NoScript are permitted. These sites can be specified individually. Users should ensure that only sites requiring JavaScript that are trustworthy are included in the list. When the user visits such a site, selecting NoScript with the right mouse button lets the user allow JavaScript temporarily or permanently for that site.