Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

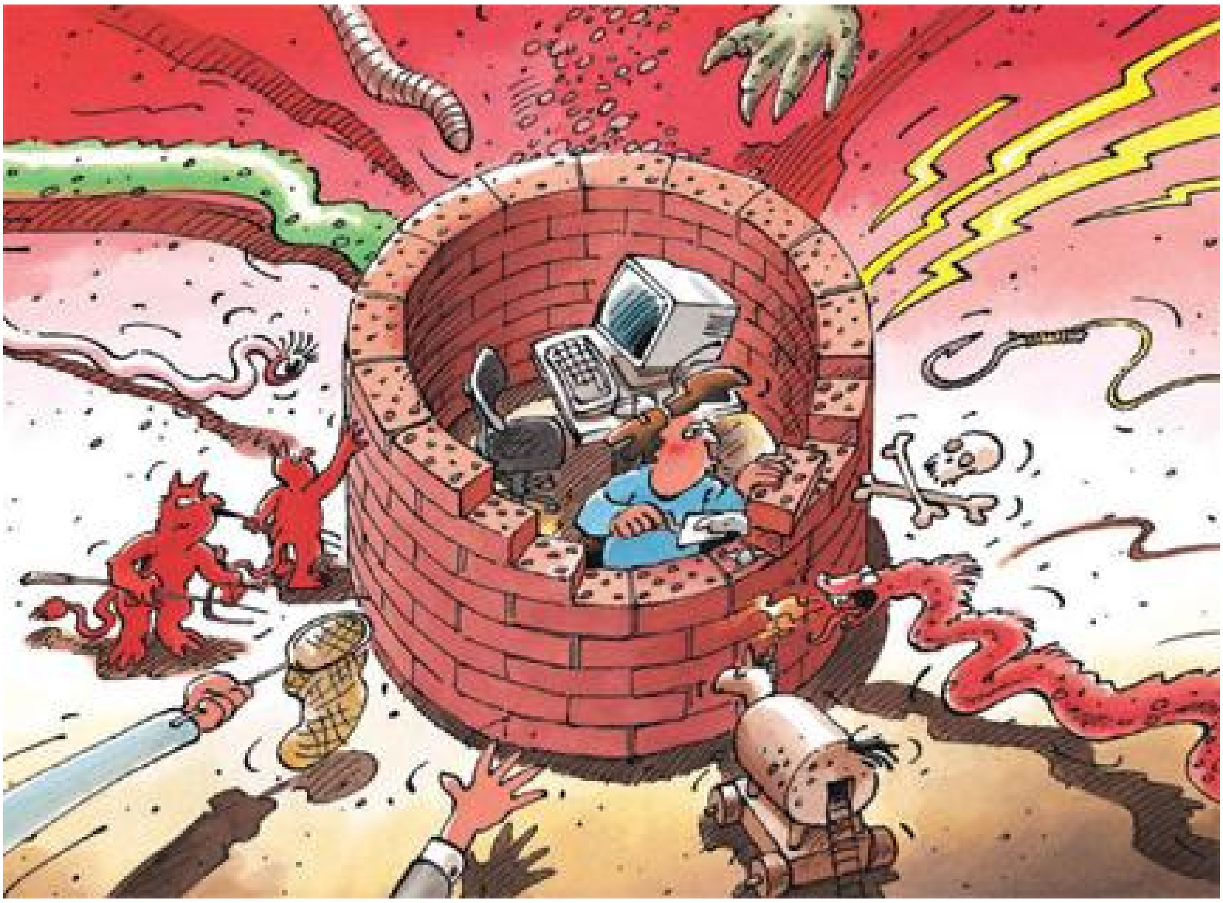
Federal IT Steering Unit FITSU
Federal Intelligence Service FIS

Reporting and Analysis Centre for Information Assurance MELANI
www.melani.admin.ch

Information Assurance

Situation in Switzerland and internationally

Semi-annual report 2013/I (January – June)



Contents

1 Focus areas of issue 2013/I

DDoS – massive attacks also in Switzerland
In the first half of 2013, the largest DDoS attack in the history of the Internet took place. The target was the non-profit organization Spamhaus, located in Switzerland. Swiss DNS servers were also misused for this DDoS attack. In January 2013, the DNS infrastructure of the SWITCH foundation was fraudulently used for an attack against third parties. MELANI indicates measures that can be taken to protect one's own DNS infrastructure against misuse in the event of a DNS amplification attack.
► Current situation in Switzerland: Chapter 3.1

- **Internet Communications Surveillance**
  One topic in particular made the headlines in the last half year: the alleged surveillance methods used by some of the intelligence services, which has been disclosed by the informer Edward Snowden. The leaks began with the NSA surveillance programme Prism, followed by publication of the methods available to the UK Government Communications Headquarters (GCHQ) to tap transatlantic deep-sea cables, and publication of a presentation of the XKeyscore analysis program.
  ► Current situation internationally: Chapter 4.1
  ► Trends/Outlook: Chapter 5.1
- **Advanced persistent threats – disclosure of numerous cases**
  In the first half of 2013, numerous targeted and professional attacks against companies and government authorities became known. Since in most cases, government actors are suspected to be behind the attacks, these attacks also gave rise to numerous political statements.
  ► Current situation internationally: Chapter 4.2
- **Content management system as a problem zone**
  The number of websites has truly exploded over the past few years. Even users without technical expertise can often place their own website on the Internet using simple means. Content management systems (CMSs) are often used for this purpose. The increasing popularity of these systems makes them interesting for cybercriminals as well, who increasingly look for and also find weaknesses in these systems.
  ► Trends/Outlook: Chapter 5.4
- **Smartphone trojans continue their advance**
  The trend of malware on smartphones continued in the last half year and has increased strongly over the past few months. The focus is especially on the Android operating system.
  ► Current situation in Switzerland: Chapter 3.3
  ► Trends/Outlook: Chapter 5.6
  ► Annex: Chapter 7.1
- **SCADA systems and industrial control systems: problem areas, vulnerabilities, attacks, and protection**
  In principle, the term "industrial control system" (ICS) can refer to any system steering and/or monitoring a physical process. While in the case of classic IT systems, where confidentiality and integrity are just as important as availability, the focus in the case of ICSs tends to be more strongly on availability.
  ► Current situation internationally: Chapter 4.5

2 Introduction

The seventeenth semi-annual report (January – June 2013) 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 summarises the activities of public and private actors. Explanations of jargon and technical terms (in italics) can be found in a **Glossary (Chapter 6)** at the end of this report. Comments by MELANI are indicated in a shaded box.

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

Chapters 3 and 4 discuss breakdowns and failures, attacks, crime and terrorism connected with ICT infrastructures. Selected examples are used to illustrate important events of the first half of 2013. Chapter 3 discusses national topics, Chapter 4 international topics.

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

Chapter 7 is an Appendix with expanded technical explanations and instructions on selected topics covered in the semi-annual report.

3 Current national ICT infrastructure situation

3.1 DDoS attacks – more numerous and intensive

Distributed Denial of Service (DDoS) attacks have remained in the focus of cybercriminals over the past few months. Different kinds of DDoS attacks can be distinguished. Some use a *botnet* consisting of infected computers (bots) or hijacked servers on the Internet. Other types of DDoS exploit poorly or insufficiently secured systems on the Internet and/or weaknesses in Internet protocols. DDoS attacks are nothing new, but they have increased in both number and intensity over the past months. While US banks continued to be in the focus of DDoS attacks (see section on "Brobot"), some Swiss companies were also targeted by DDoS attacks. This will be discussed in the chapters below.

Largest DDoS attack in history against Spamhaus

In the first half of 2013, the largest DDoS attack in the history of the Internet so far occurred. The target was the non-profit organization Spamhaus located in Switzerland[1], which is dedicated to combating spam and other threats in cyberspace.

In March 2013, unknown perpetrators launched a massive DDoS attack against the Spamhaus website. The attack continued for several days, reaching a data volume of 300 Gbps at its peak, which corresponds to the data content of over 50 CDs – per second. Spamhaus turned to the cloud provider CloudFlare, which tried to defend against the attack. CloudFlare's defensive measures were countered by an attack against London Internet Exchange LINX, so that all data traffic processed via that exchange was severely disrupted for a short period of time[2].

This DDoS attacks was a *DNS amplification attack*. Bogus *DNS* queries were sent to open DNS servers on the Internet ("*open DNS resolvers*")[3]. Since the DNS queries were bogus, containing the source IP address of Spamhaus, this caused the open DNS servers to send their responses to Spamhaus's IP address rather than to the actual sender of the *data packet*. Since a response to a DNS query is typically many times larger than the DNS query itself, the attacks were able to generate a considerable network load of up to 300 Gbps with relatively little bandwidth.

[1] The Spamhaus Project: http://www.spamhaus.org/ (as at 31 August 2013).

[2] The Verge - Spam war caused failure at critical internet exchange center: http://www.theverge.com/2013/3/28/4156570/Dutch-spamhaus-DDoS-took-down-london-internet-exchange (as at 31 August 2013).

[3] For Information on the number of *Open DNS resolvers* in the Swiss AS see: http://securityblog.switch.ch/2013/05/02/ddos-and-open-resolvers-the-swiss-view/ (Stand: 31. August 2013).

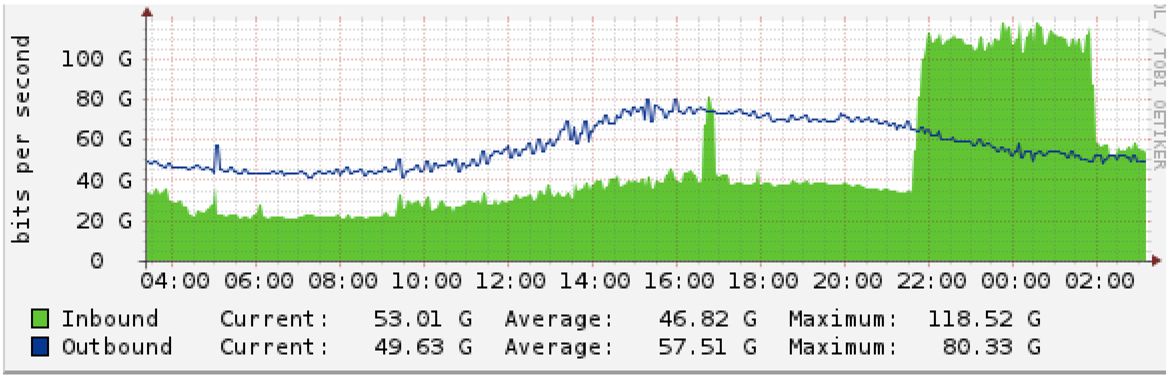


Figure 1: Network traffic before, during, and after the DDoS attack (source: CloudFlare)

Some sources suspected that the attack was so large that it temporarily disrupted the entire Internet. MELANI was unable to confirm these suspicions, however, and at least in Switzerland was unable to observe any disruption of the Internet.

The following measures can be taken to protect one's own DNS infrastructure from being misused in the event of *DNS amplification attacks*:

Preventing IP address spoofing:

It must be ensured that devices on the Internet be unable to send data packets with an arbitrary sender IP address (*IP address spoofing*). For this purpose, a Best Current Practice (BCP38) was developed in 2000 and published under RFC2827. Although this standard is already more than a decade old, most *Internet service providers (ISPs)* have still not implemented it fully or even at all.

To prevent or minimize the possibility of Swiss ICT infrastructure being used for this type of DDoS attack, MELANI recommends that all Swiss Internet service providers implement the standard (BCP38) described in RFC2827 across the board in order to prevent IP address spoofing.

Securing DNS servers:

Another measure to minimize or weaken DNS reflection attacks in future is to secure DNS servers. Many (DNS) servers, but also other network peripheral devices are connected to the Internet using a standard configuration (usually the device's factory settings). Such standard configurations are often unsecure and not restrictive enough. Specifically, for instance, these devices accept queries from the entire Internet. Devices and software should be configured so that they only accept queries from the local or a limited IP address range. This helps prevent the devices from being misused by criminals for attacks against third parties on the Internet.

MELANI recommends that operators of DNS servers or devices making a DNS service available to comply with or implement the following standards and best practices:

1. RFC 5358 (BCP140) Preventing Use of Recursive Nameservers in Reflector Attacks: http://tools.ietf.org/html/bcp140
2. Windows 2003 Server – Securing DNS: http://technet.microsoft.com/en-us/library/cc785404%28v=ws.10%29.aspx

3. Secure BIND Configuration Template:
   http://www.cymru.com/Documents/secure-bind-template.html
4. Deactivation of DNS Recursion (if not needed):
   http://www.team-cymru.org/Services/Resolvers/instructions.html
5. Implementation of Response Rate Limiting:
   http://www.redbarn.org/dns/ratelimits

Swiss DNS servers misused for DDoS attack

Swiss DNS servers were also misused for DDoS attacks. In January 2013, the DNS infrastructure of the SWITCH foundation, which runs the top level domains (TLDs) ".ch" and ".li", was misused for a *DNS amplification attack* against third parties[4]. With only minimal bandwidth on their part, the attackers were able to generate a high load on the DNS infrastructure, flooding the target of the attack with up to 500 Mbps.

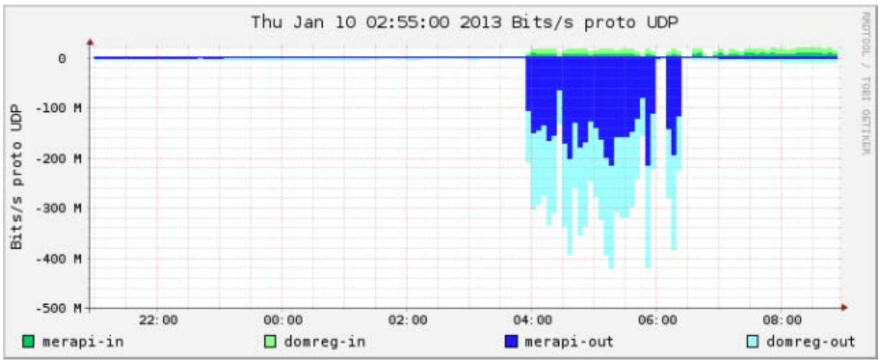


Figure 2: Network traffic before, during, and after the DDoS attack (source: SWITCH Security Blog)

Since SWITCH's DNS infrastructure is designed for high volumes of data traffic, the misuse of the infrastructure had no impact on the top level domains ".ch" and ".li". According to SWITCH, this DNS amplification attack succeeded in generating responses of up to 225 MBps with a bandwidth of only 3 MBps. This means that merely a standard DSL or cable connection (along with the requisite know-how) is necessary to launch such an attack. This example shows with how little effort a DDoS attack is possible nowadays. Thanks to SWITCH's good reaction, the misuse could be stopped within a very short period of time.

DDoS with Brobot also in Switzerland

In the last MELANI Semi-annual report, we reported on DDoS attacks against US banks[5]: The websites of several US banks were disrupted using DDoS attacks with data volumes of up to 60 Gbps and were even shut down. It is suspected that Iran was behind these attacks.

The attacks are carried out with the help of compromised webservers. For this purpose, the attackers search the Internet for vulnerable Joomla![6] installations. If the attackers' search is

[4] SWITCH Security Blog - CH-Zone Opfer eines DNS-Amplifikations-Angriffes: http://securityblog.switch.ch/2013/01/10/ch-zone-dns-angriff/ (as at 31 August 2013).

[5] MELANI Semi-annual report 2012/2, Chapter 4.2.1: http://www.melani.admin.ch/dokumentation/00123/00124/01535/index.html?lang=en (as at 31 August 2013).

successful, a known vulnerability in Joomla! is exploited to place *malware* on the victim's website. The malware is a malicious *PHP script* called Brobot[7], which opens a backdoor to the system and has DDoS functionality. From the perspective of the attackers, hacked webservers offer a great advantage: Webservers often have a higher bandwidth at their disposal than normal Internet connections, which is why already a small number of bots can be sufficient to launch effective DDoS attacks.

Swiss websites are also affected by Brobot. In the first half of 2013, MELANI informed dozens of operators of websites infected with Brobot:

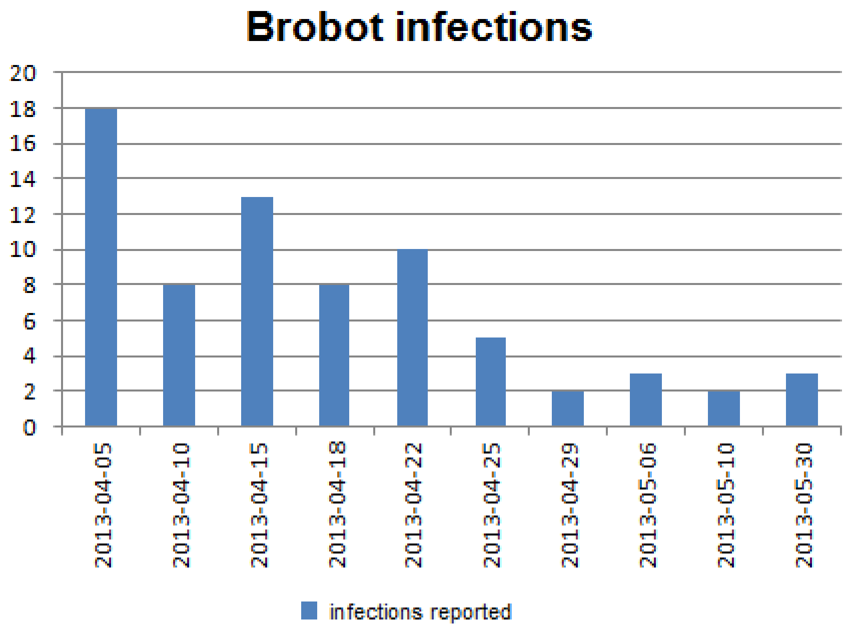


Figure 3: Brobot infections reported by MELANI

The affected owners of the websites and the web hosting providers were informed by MELANI of the infections. However, not all operators reacted – some websites remained infected for several months and were regularly misused for DDoS attacks against US banks.

3.2 Phishing trends

Again in the first half of 2013, numerous phishing attempts were observed. The trend that also e-banking clients of smaller banks are being targeted by attackers has continued. Apparently, it is worthwhile for the scammers to configure and adapt systems especially for

[6] Joomla! is a popular content management system.

[7] Symantec - PHP.Brobot: http://www.symantec.com/security_response/writeup.jsp?docid=2013-011012-0840-99&tabid=2 (as at 31 August 2013).

these targets, even if they statistically speaking can only count on one or two potential victims at the financial institution in question.

Making deactivation difficult

Various techniques used by criminals to make it more difficult for administrators to deactivate the phishing sites have already been discussed in a previous semi-annual report.[8] A new technique was observed in the current reporting period. In this case, the display of the phishing site depended on the time zone setting in the browser. If the time zone was Central European Time, a phishing attempt was made – in every other time zone, an error message was displayed. The purpose of this was of course to make (e.g., American) providers think that the site had already been removed, so that no further action would be necessary. This meant that fraudulent sites remained online longer and could potentially catch more victims.

Phishing site against Swiss financial institution using Flash for the first time

Normally, the scammers copy the original webpage of the bank when creating their phishing sites, making a few small changes and then saving them on a server that has been prepared for the scam. This process is relatively simple and does not require substantial ICT expertise. Astonishing is that for the first time, a phishing site using *Flash* was discovered that targeted a Swiss financial institution. It can only be speculated why the scammers employed this relatively complicated programming method. Data found in the directory of the phishing site lend to the conclusion that the scammers used a simple kit for preparing website forms that generated Flash versions. Another possible reason could be that the text in these Flash programs cannot be searched. Anti-phishing programs then have fewer possibilities to recognize a phishing site using keywords and to warn the computer user.

Also e-banking clients of smaller banks affected

It is increasingly being observed that, in addition to the numerous phishing attempts against credit card companies and major banks, smaller banks have recently also been affected by phishing. One reason is probably that the scammers are moving to these financial institutions in the hope that the security measures are not as high, or that clients have not been confronted with this phenomenon as frequently.

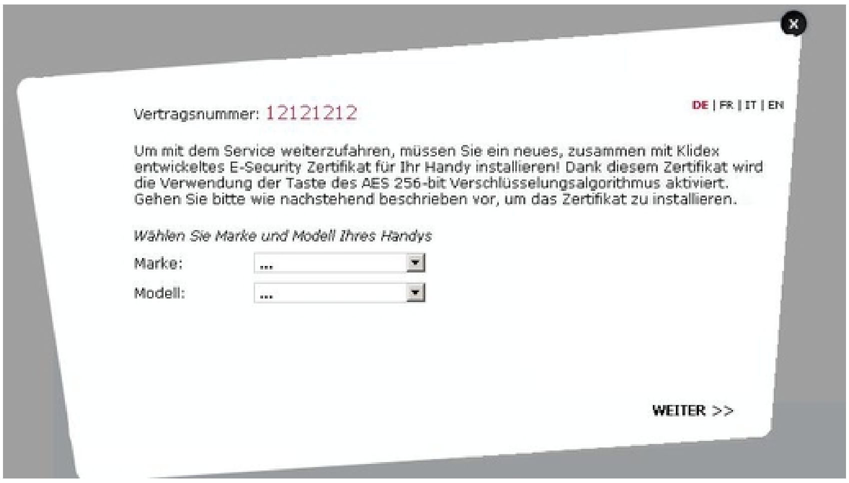
Purely statistically speaking, an attack against smaller banks would only make sense if the database of the attackers is excellent and clients only of that bank are targeted with phishing messages. So far, this kind of targeted approach to smaller banks has not been observed – the circulation and sending of phishing e-mails appears to continue to be on a rather random basis.

3.3 Circulation of e-banking malware on smartphones

In the first half of 2013, the Reporting and Analysis Centre for Information Assurance (MELANI) warned against a new wave of attacks against Swiss e-banking business using

[8] MELANI Semi-annual report 2011/2, Chapter 3.4: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=en (as at 31 August 2013).

SMS transaction signing. This type of attack installed malware on a computer. When a client logs on to the e-banking account, a message appears claiming that a new e-security certificate has to be installed. The client is asked to enter his or her smartphone model and mobile telephone number. The client is then requested by SMS to install the new certificate on the smartphone. In fact, however, malware is then installed on the device allowing the attackers to intercept the SMS necessary for transaction signing and to carry out fraudulent payments.



Vertragsnummer: 12121212

Um mit dem Service weiterzufahren, müssen Sie ein neues, zusammen mit Klidex entwickeltes E-Security Zertifikat für Ihr Handy installieren! Dank diesem Zertifikat wird die Verwendung der Taste des AES 256-bit Verschlüsselungsalgorithmus aktiviert. Gehen Sie bitte wie nachstehend beschrieben vor, um das Zertifikat zu installieren.

Wählen Sie Marke und Modell Ihres Handys

Marke: ...

Modell: ...

Figure 4: Window displayed during the login process, asking the e-banking client to install a certificate on the smartphone.

Swiss banks never use screen displays or SMSs to ask clients to install new security elements on their devices. MELANI recommends that all e-banking clients asked during an e-banking session to install a certificate (see picture) or the like on their smartphone to interrupt the e-banking transaction, close the connection to e-banking (logout button), and to contact the bank immediately. A detailed description of the attack can be found in Annex 7.1.

3.4 Targeted social engineering attacks against Swiss companies

Targeted fraud attempts use various social engineering methods. These attacks are more and more frequently directed against small and medium enterprises (SMEs).

Two cases reported to MELANI against Swiss companies will be discussed here. In the first case, which took place in March 2013, the chief financial officer of an internationally operating SME received an e-mail supposedly sent to him by the CEO. This e-mail looked just like the e-mails usually sent within the company and requested the chief financial officer to transfer a large sum of money to the account of a lawyer for a supposed acquisition in China. The project was of course fictitious, and all of this was just a scam to receive transfer of the payment.

Especially interesting in this case is the relatively large amount of research the perpetrator had to carry out in advance. In order to even set up a corporate scenario like this, the scammers had to research and analyse the company's organizational structure.

In June 2013, another attack against a Swiss SME was reported to MELANI. An unknown perpetrator tried to penetrate the corporate network of that company in the canton of Zurich. For this purpose, the perpetrator called an employee of the company and asked to discuss an open invoice with the accounting department. Since the accounting employee was unable to find the invoice in the system, the attacker – who spoke French – offered to scan in the invoice and send it by e-mail. The employee gave the attacker her e-mail address and, as discussed by telephone, received an e-mail with a *hyperlink* just a few minutes later. But after she clicked on the link, she received an executable Windows file ending in ".exe" instead of the expected invoice. When the file was executed, a *remote administration tool (RAT)* was installed unnoticed on her computer. This tool allowed the attackers to control the computer remotely via the Internet without being detected.

Fortunately, the employee became suspicious and reported the suspicious e-mail to the company's ICT support department, which was able to confirm the infection of the computer and render it harmless. The company then filed criminal charges against the unknown perpetrators. Also in this case, MELANI assumes that the attackers had a financial motive.

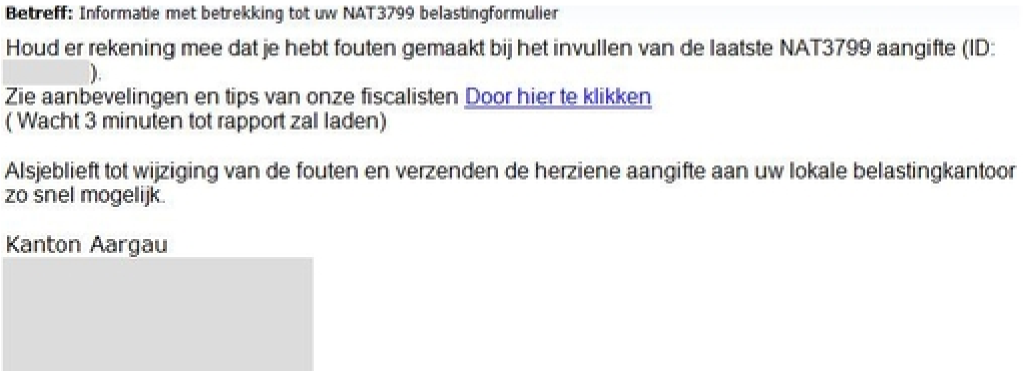
In recent years, such targeted attacks against Swiss companies have increased. The example shows that not only major corporations are being affected by these attacks, but also small and medium enterprises. The attackers pursue different goals in these attacks. Often, however, they have financial motives (e.g., e-banking fraud) or business interests (obtaining information on competitors, information on client base, industrial espionage).

Such attacks are often realized using a *remote administration tool (RAT)*. This is malware that can be acquired on the Internet for a few hundred dollars, offering a wide range of functions (from recording keystrokes to complete remote control of the computer). As a rule, such RATs are not as technically sophisticated as e-banking trojans and other malware. Nevertheless, many anti-virus programs do not recognize malware like this, or only after it is too late.

3.5 Circulation of e-mails with links to infected sites

E-mails trying to get the recipient to click on something are widespread. Already in the last semi-annual report[9], MELANI discussed e-mail with fictitious invoices or transactions trying to induce the recipient to click on an attachment. The attachment contains malware, usually packed into a *zip* file, that infects the computer when it is opened. A slightly different kind of attempt was observed on 22 January 2013. An e-mail in Dutch pretended to be from a public authority of the Canton of Aargau. When the link was clicked on, an attempt was made in the background to find vulnerabilities on the computer and install malware. The Canton of Aargau was not the victim of a hacker attack – the message was merely sent from bogus e-mail addresses using the "ag.ch" domain. It is often observed that well-known companies or authorities are misused as senders.

[9] MELANI Semi-annual report 2012/2, Chapter 3.2: http://www.melani.admin.ch/dokumentation/00123/00124/01535/index.html?lang=en (as at 31 August 2013).



Betreff: Informatie met betrekking tot uw NAT3799 belastingformulier

Houd er rekening mee dat je hebt fouten gemaakt bij het invullen van de laatste NAT3799 aangifte (ID: [redacted]).
Zie aanbevelingen en tips van onze fiscalisten Door hier te klikken
(Wacht 3 minuten tot rapport zal laden)

Alsjeblieft tot wijziging van de fouten en verzenden de herziene aangifte aan uw lokale belastingkantoor zo snel mogelijk.

Kanton Aargau
[redacted]

Figure 5: E-mail with link to drive-by infection

It is unclear why the e-mail was written in Dutch. But it can be assumed that the attackers made a mistake, since this fact significantly diminished the chances of success. It is also unclear why a public authority of the Canton of Aargau was used as the sender. Nevertheless, it should once again be pointed out that especially unexpected e-mails from known companies and authorities should always give rise to caution, since the sender e-mail addresses can be falsified very easily. The fact that in this case, the infection exploited a vulnerability on the computer shows how important it is to keep all applications updated in addition to the operating system.

3.6 VoIP: Fraudulent use in Switzerland

VoIP (Voice-over-IP) is the term for the technology used to make phone calls over IP networks, either on a private, controlled network or the public Internet. In recent years, VoIP telephony especially over the public Internet has increased strongly among individuals and businesses. One of the main reasons for the increasing popularity is the inexpensive price especially for international calls. But with the rising popularity of this technology, there has also been an increase in abuse.

In the first half of 2013, the Reporting and Analysis Centre for Information Assurance (MELANI) got the information on a large-scale fraud in which the infrastructure of a Swiss company, or more precisely a virtual server of that company, was used to make calls to premium numbers (*VoIP toll fraud)*. In return for this very lucrative business, the hacker receives a commission from the operator of the premium numbers.

In this case, the virtual server was hacked and misused to perpetrate the fraud. Most probably, the accounts located on the servers were also hacked, and the costs for the calls to these premium numbers were charged to the actual holder of the telephone account in question, either an individual or a business.

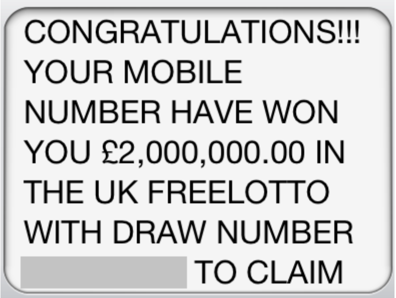
Fraud perpetrated in whole or in part by telephone now largely relies on VoIP technology. This is especially true of voice phishing, in which victims are called to induce them to divulge their e-banking access data. Also callers who purport to be Microsoft support desk employees and try to gain access to computers citing a supposed security problem make use of this technology. This also means an increasing focus on the security of this technology. For the perpetrators, the use of hacked infrastructure has various advantages: First of all, they are able to make phone calls at the expense of others, but they are also better able to conceal their identity. In addition to these scams, other possible abuses of VoIP are discussed in Chapter 5.7.

3.7 SMS wave with advance payment fraud

Users have long become accustomed to e-mail *spam*. Providers do their best to filter and remove these undesired messages. It is only a logical consequence that this type of attack would sooner or later resort to *SMSs* as a dissemination channel. Until now, sending SMSs has required too much of an effort compared to sending spam e-mails, however. But this now appears to be changing, as a first case in the first half of 2013 shows.

In April 2013, an SMS spam wave flooded Switzerland as well. More than 500,000 Swisscom customers, but also numerous Orange and Sunrise customers, were hit by this wave. The message was apparently sent to random recipients within well-known ranges of phone numbers.

The SMS in this case involved typical advance payment fraud. The offers and promises made in messages like this – in this case a lottery win – are simply made up and intended to create a more or less credible background against which the fraud can then be perpetrated. If the recipient responds to the message, some excuse is made to request an advance payment. The promised money is never transferred, however. At the same time, personal data (passport number, photographs, etc.) that may be provided can be misused as a false identity for further scams.



CONGRATULATIONS!!! YOUR MOBILE NUMBER HAVE WON YOU £2,000,000.00 IN THE UK FREELOTTO WITH DRAW NUMBER [redacted] TO CLAIM

Figure 6: SMS involving advance payment fraud

The SMSs were sent via the British telephone providers T-Mobile UK and Orange UK. Swisscom has stopped forwarding SMSs from these two providers until they were able to stop or block the SMSs in their own networks.

SMS spam messages are not as widespread as e-mail spam, which makes up – depending on the source – from 70%[10] to 85 %[11] of all e-mail messages sent. There are also regional differences in the volume of SMS spam. In the United States, SMS technology is not as pop-

[10] http://www.spamfighter.com/News-18508-Spam-Increases-to-707-of-Total-E-mail-Traffic.htm (as at 31 August 2013).

[11] http://senderbase.org/static/spam#tab=1 (as at 31 August 2013).

ular. Accordingly, the SMS spam rate is less than 1%. In Asia, the spam rate is up to 30%.[12] SMS spam requires more of an effort than e-mail spam and is therefore not yet really interesting for spammers. However, the increase in smartphones in conjunction with the possibilities for hacking such phones will also have an effect on the volume of SMS spam sent.

The possibility of filtering SMS spam is not yet very advanced and usually works on the basis of black lists, as opposed to spam e-mails, which are filtered using a *spam score*.

3.8 Advertising monitor administered by third party

A special operation took place in June 2013. In a post box office in Zurich a few youngsters tampered with an advertisement screen. In this particular post box office the Swiss Post is renting out floor space to an external advertising company in order for them to exhibit advertisement screens. The entire operations and maintenance is performed by the tenant (in this case the advertising company).

A 17-year-old managed to log onto the system by removing the physical security elements and restarting the computer, which was attached to the screen. He then installed a tool, which enabled him to upload pornographic material to that particular screen from different locations. The point of this action was to draw attention to the security vulnerability. The campaign, which was picked up by the press and television caused nationwide attention.

In addition to the legal questions in this case – namely that making pornographic material available to minors is punishable – this incident also raises the question of the best course of action when a vulnerability is found. It must be considered to what extent an action like this really raises awareness, or whether it simply serves personal gratification, and whether it would be more efficient to inform the office concerned directly.

More and more frequently, the identification of vulnerabilities also serves financial motives. The market in the security business is hard-fought. There are companies specializing in finding vulnerabilities and selling them to the manufacturers. Finding and publishing vulnerabilities is also used as an opportunity to draw attention to one's own company's professionalism.

3.9 Swiss Cyber Storm and the cyber talents of tomorrow

On 13 June 2013, the Swiss Cyber Storm 4 conference took place at the KKL Luzern. A broad field of international speakers with outstanding expertise addressed their talks primarily to decision-makers in the Swiss business world.

Apart from this, the conference sought out the best Swiss cyber talents. In the weeks before the all-day congress, university and secondary school students had the opportunity to take part in "Challenges" online. The goal was to solve cyber puzzles or brain twisters. The search was not for hackers, but rather for talents who think further and more globally than hackers. Specifically, this means that it was not enough to be able to crack encrypted zip files, for example. Rather, the candidates had to identify the error in the encryption they used to crack

[12] http://en.wikipedia.org/wiki/Mobile_phone_spam (as at 31 August 2013).

the files – and how they would fix the error. So the purpose was not simply to attack, but rather also to show how the systems could be protected.

The demands on the participants were extremely varied. In addition to the technical challenges, they also had to solve them within a certain time limit, which further increased the pressure on the participants. This called for the ability not only to think within established paths, but rather also to react flexibly and to work in a solution- and team-oriented way.

Swiss Cyber Storm was a gain for all participants: They were able to expand their knowledge and also make important contacts with the private sector. One of the participants has already received a job offer, for instance.

What happens after Swiss Cyber Storm?

The winning group cannot rest on its laurels. It was invited by the organizers of Swiss Cyber Storm to compete against the winning team of the Austrian sister conference in a final to be held in Linz in November 2013.[13]

Together with Swiss Police ICT – a private association that has built a bridge between the IT world and criminal prosecutors for several years – MELANI has assumed patronage of Swiss Cyber Storm. The shared goal is to continue to find new Swiss cyber talents in future.

4 Current international ICT infrastructure situation

4.1 Internet Communications Surveillance

One topic in particular made the headlines in the last half year: the alleged surveillance methods used by some of the intelligence services, which has been disclosed by the informer Edward Snowden. The leaks began with the NSA surveillance programme Prism, followed by publication of the methods available to the UK Government Communications Headquarters (GCHQ) to tap transatlantic deep-sea cables, and finally publication of a presentation of the XKeyscore analysis program. Snowden was an employee of the CIA before he switched to the private security provider Booz Allen Hamilton, one of whose clients was the NSA.[14] In the course of these disclosures, surveillance programmes have also been discussed in several other countries.

Prism

Prism is the name of an alleged surveillance programme of the NSA disclosed by Edward Snowden. It is called Prism because a prism is allegedly used to separate out and transmit signals in fibre optic cables. It is questionable, however, whether the data are really gathered in this way. More likely is that the surveillance programme is a project used by the NSA to gain access to the servers of different US companies such as Microsoft, Google, and Yahoo.

[13] http://www.verbotengut.at/ (as at 31 August 2013).

[14] This report covers the reporting period from January to June 2013. Other information that has become public on the informer Edward Snowden will be discussed in the next semi-annual report.

The fact that government offices have access to domestic telecommunication infrastructure is nothing unusual. However, such access is generally strictly regulated: To obtain such data, criminal proceedings are typically necessary, along with a court order or other reasons set out by special legislation. What is new about the disclosures is that the US intelligence services are alleged to have not only selective access to specific data, but rather have systematic and comprehensive access to telecommunication data. All companies mentioned in this connection have denied that such comprehensive cooperation exists, and they have stated that they release data only pursuant to court orders relating to specific accounts.

The government side in turn has always stated that all surveillance measures are authorized by law and have been approved by the three branches of the US government. The Foreign Intelligence Surveillance Act (FISA) adopted in 1978 governs surveillance abroad, of foreign persons on US territory, and of US citizens. The Foreign Intelligence Surveillance Court (FISC) is the judicial authority responsible for authorizing surveillance measures to this effect. Amendments to the FISA through enactments such as the Patriot Act (2001) and the Protect America Act (2007) have granted the authorities far-reaching powers to monitor communications and have adjusted those powers in response to changing threats – especially terrorism – and technical developments such as the Internet as a medium and the shift of international communications from satellites to fibre optic cables.

Tempora

Another report given to the British newspaper "The Guardian" by Snowden refers to a surveillance programme called Tempora, which is said to be operated by the British intelligence service. This programme is alleged to give the UK Government Communications Headquarters (GCHQ) access to transatlantic data cables, enabling it to siphon off and copy the desired data. The focus of the report was on the TAT-14 cable, which runs from Germany, Denmark, the Netherlands, and France via the United Kingdom to New Jersey. The GCHQ is claimed to have access to the connection at the port town Bude, whether the cable lands in the UK. The tapped data is said to include e-mails, Facebook entries, but also telephone conversations. The GCHQ is claimed to be tapping more than 200 fibre optic cables and employing 500 people to analyse the tapped data.[15]

Transatlantic Internet communications have shifted more and more to deep-sea fibre optic cables in recent years. While 80% of transatlantic data communications were via satellite in 1986, the bulk – both within and between continents – now goes through fibre optic cables, which are connected to a network. There are usually several possible paths for communication between two users, and only when the data is actually transmitted is the path decided. If data communications are tapped from a deep-sea cable, this does not necessarily mean that the entire communication, e.g., a complete e-mail message, can be intercepted, even though this may often be the case in practice.

XKeyscore

XKeyscore is an analysis software program developed by the NSA and said to be used by various intelligence services. It is said to make it possible to assign a wide range of data in various databases, including e-mails, online chats, etc., to a target person in real time. Dif-

[15] http://www.handelsblatt.com/politik/international/abhoerskandal-auch-britischer-geheimdienst-spaeht-daten-aus/8391120.html (as at 31 August 2013).

ferent criteria such as *IP addresses*, languages, browsers, settings, and telephone numbers can be queried. The goal is to be able to find all data gathered in this connection. According to the secret presentation from the year 2008 published by Snowden, the XKeyscore network consists of more than 700 data servers spread about 150 locations around the world. The foreign intelligence services of the UK, Canada, Australia, and New Zealand are alleged to be participating in XKeyscore. The German Federal Intelligence Service (BND) is also claimed to be using the program.[16]

It is not surprising that intelligence services have tools suitable for the efficient analysis of data already gathered. The analysis of large data volumes can only be accomplished with suitable analysis programs nowadays. Everyone knows how search engines work: Even here, it is crucial to find the desired results within split seconds. Apart from the question of who has access to what data in such a system at what times, the focus should not be on how an intelligence service analyses data, but rather what data an intelligence service is allowed to be gathering and storing in the first place, and what queries are actually permissible in regard to this data.

4.2 Advanced persistent threats: Red October, Net Traveller, MiniDuke

In the first half of 2013, numerous targeted and professional attacks against companies and government authorities became known. Most of these attacks were *advanced persistent threats (APTs)*. APTs are characterized by the persistent and varied attempts by attackers to enter certain systems in order to set themselves up there for an extended period of time and unfold their malicious activities undetected. Often, the original infection is accomplished using *spear phishing* or *watering hole attacks*. Subsequently, backdoors are set up and administrator rights are obtained by devious means. The ultimate goal is to remain undetected in the network for an extended period of time, to move around unnoticed, to spy out data, and in some cases also to change or delete data. To carry out such attacks successfully, considerable effort is needed, which is why government actors are often suspected of being behind them. But also criminal groups or individuals with a lot of time, a lot of motivation, and the prospect of selling the collected data to third parties cannot be ruled out as perpetrators.

In a report, the ICT security firm FireEye estimates that companies and organizations receive an e-mail with a malicious link or attachment every three minutes.[17] Also in Switzerland, systems with sensitive information are exposed to such attacks on a daily basis.

In the first half of 2013, reports about such attacks emerged in rapid sequence. Since government actors are generally suspected of being behind these attacks, the attacks also gave rise to numerous political statements.

[16] http://www.zeit.de/politik/deutschland/2013-08/bnd-xkeyscore-nsa (as at 31 August 2013).

[17] http://www2.fireeye.com/WEB2012ATR2H_advanced-threat-report-2h2012.html (as at 31 August 2013).

January: Operation Red October

On 14 January 2013, the Russian ICT security firm Kaspersky gave details regarding a spy operation against diplomatic missions, governments, and international organizations. The targets of the operation called Red October were primarily in Eastern Europe, Central Asia, and the CIS countries. The Kaspersky report also noted that numerous Swiss IP addresses were being used to access *command-and-control server infrastructure*, which at first glance indicated that many victims were in Switzerland. In an initial analysis, MELANI found that most of these were dynamic IP addresses. After eliminating the multiple counts of suspected cases, the number of effective infections was corrected significantly downward to five victims. The affected victims were also not Swiss organizations, but rather foreign infrastructures operating in Switzerland.

The victims were infected using malware in e-mail attachments. One special feature of these attacks was that the malware was able to obtain data not only from infected computers, but also from mobile devices. This spy operation is claimed to have been operating since at least 2007. According to Kaspersky, the perpetrators are Russian.

February: APT1

At the beginning of this year, attacks targeting US companies experienced an especially strong increase. This series of attacks led to numerous statements by high-ranking US politicians calling for stronger defences and often accusing China as the country posing the greatest threat in the field of cyber espionage.

Despite the diversity of the attacks and targets, certain patterns can be recognized. The attacks mainly targeted American Internet companies such as Apple, Facebook, Google, Microsoft, and Twitter. The systems were infected mainly using *watering hole attacks*, generally via a website for developments of mobile applications. The visitors to this site were infected using a *zero-day exploit* in the *Java* program. At the same time, many major American media outlets (New York Times, Wall Street Journal, Bloomberg, Washington Post) reported attacks especially on e-mail accounts of their journalists. In both cases, China was repeatedly suspected of being behind the attacks.

In this context, the American security firm Mandiant published a report in February 2013 claiming to be able to show the participation of the Chinese government in cyber espionage operations against the United States and some European countries. The report was based on research in collaboration with the targeted companies. As its most important conclusion, the report made a link between a group of cyber perpetrators called "APT1" and a unit of the Chinese army. Mandiant claimed that the group had stolen high volumes of data from 146 selected victims since 2006.

Also in this case, Switzerland was affected only indirectly, since the targeted systems were foreign infrastructures operating in Switzerland.

February: Operation Beebus

In the same political context, the American company FireEye published the results of its work on another espionage affair, an APT called Beebus, in February 2013. Beebus appeared to be targeting companies especially in the defence and aerospace sectors. The victims were infected both using targeted e-mails and *drive-by* downloads. According to FireEye, the first traces of the attack go back to 2011. FireEye suspects that the attack might be of Chinese origin. No targets in Switzerland are known.

February: MiniDuke

Also in February 2013, Kaspersky reported on a sophisticated attack using the MiniDuke malware. The target appears to have been primarily government structures and other victims all located in Europe. The victims were infected using *spear phishing* and prepared PDF documents. A special characteristic of this attack is the use of Twitter accounts as generators of the *domain names* of the *command-and-control servers*. According to current knowledge, no infrastructure in Switzerland was affected.

June: NetTraveler

At the beginning of June 2013, Kaspersky published details on NetTraveler, a series of malware used for APT attacks. 350 victims in 40 countries were affected; however, there is currently no indication of any connection with Swiss infrastructures. The targets were in the industrial, energy, communication, new technologies, and government sectors. Interestingly, according to Kaspersky, six targets were simultaneously affected by NetTraveler and Red October. However, this finding alone does not lend itself to the conclusion that both attacks can be traced back to the same (or to different) perpetrators.

The many reports by security firms, victims, and authorities have again put cyber espionage and APT attacks into the limelight. Targeted espionage attacks are no longer isolated events or isolated groups of espionage cases, however. Rather, there is continuous interest and accordingly continuous pressure on sensitive data. Switzerland is also affected by this, since a large number of top companies are located here that have high-value know-how and information. In addition to the usual and necessary technical security measures, organizational measures are also necessary. Moreover, prevention must as a matter of principle and independently of recent incidents always have a high priority and, for instance, be accomplished by raising the awareness of employees, who among other measures must be trained to deal with e-mails cautiously.

The attacks can only rarely be attributed to a specific perpetrator. Geographically, they may well be localized quite precisely. But only in the rarest cases can it be shown without a doubt that the government in question is responsible for the attacks.

It is also interesting that in some of these attacks, infrastructures were used that are known in connection with criminal activities. Apparently, criminal infrastructures are being employed not only for financial enrichment, but also act in the interest and in the pay of individual governments and their espionage motives.

4.3 Korea conflict in cyberspace

In the first half of 2013, the conflict in Korea worsened. After indications of nuclear weapons tests by North Korea[18] and the subsequent tightening of UN sanctions against North Korea, North Korea announced that it was now at war with South Korea, and it for the first time also threatened a preventive nuclear strike against the United States. This centre of conflict also had various cyber components. The official North Korean news agency KCNA, for instance,

[18] http://www.seismologie.bgr.de/sdac/erdbeben/kernexplosion/nkorea_20130212_deu.html (as at 31 August 2013).

reported on a local outage of the Internet due to an enemy computer attack on 14 March 2013. The United States and South Korea were accused by North Korea of having caused this outage. What exactly happened could not be determined. In North Korea, only a small proportion of the population has access to the Internet. Just a few days later, on 20 March 2013, a massive cyber attack was launched against South Korea, affecting three South Korean television stations and two financial institutions. The victims were unable to restart their computers, since the hard discs had been deleted by the malware. While some cash machines, *points of sale*, and the *mobile banking* of the targeted banks broke down, the television programmes of the targeted stations were not affected. Additionally, website defacements were perpetrated by a group named «Whois Team», who used this method to communicate that this would be only the beginning of its actions: «All data are in our hands, unfortunately we have deleted your data». Another group called «New Romanic Cyber Army» has plead guilty to this attack and claims to have leaked all collected information from banks and media. McAfee has published a report stating that these attacks had close links to a hitherto unknown espionage campaign against the South Korean Army, which supposedly has been active since 2009. This espionage campaign, which was called «Operation Troy» searched computers for certain keywords in the military domain. [19] Hence, the hacking activities could have been a diversion from these espionage activities.

On 25 June 2013, the 63rd anniversary of the beginning of the Korean War, another attack occurred – this time in the form of a DDoS attacks against *DNS servers* of the South Korean government. Official websites, including of the office of the president, were no longer reachable. Representatives of the Anonymous movement, which was mentioned by several sources as the perpetrator, distanced itself from the attacks. The South Korean side accused North Korea of being responsible for both the attacks in March and for those in June. North Korean IP addresses and malware patterns were presented as possible proof.[20]

After this last attack, also Symantec published a report[21] according to which there were clear indications that one of the *DDoS attacks* on 25 June 2013 was connected with the various attacks over the past four years against South Korea, including the attacks of July 2009 and March 2011[22], and that they could be attributed to the Group "DarkSeoul". Symantec suspected that the group consisted of 10-50 people who could also be linked to the e-banking *malware* Castov. The group is claimed to have been involved in attacks against the United States as well. Determining the origin of the attacks and attributing them to a potential government act is very difficult however, as experience has shown.

4.4 Twitter account of Associated Press hacked

The social network Twitter was targeted more frequently by attackers in the first half of 2013. The most serious case occurred on 23 April 2013, when the Twitter account of the Associat-

[19] http://blogs.mcafee.com/mcafee-labs/dissecting-operation-troy-cyberespionage-in-south-korea (as at 31 August 2013).

[20] http://www.csoonline.com/article/736531/south-korea-blames-north-korea-for-cyberattacks (as at 31 August 2013).

[21] http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war (as at 31 August 2013).

[22] MELANI Semi-annual report 2009/2, Chapter 4.2: http://www.melani.admin.ch/dokumentation/00123/00124/01109/index.html?lang=en (as at 31 August 2013).

ed Press (AP) was compromised. Hackers had gained access to AP's Twitter account and published a tweet in its name claiming that there had been two explosions at the White House and that President Obama had been injured. Nearly 2 million users followed this tweet. US markets were temporarily affected. Within three minutes, the American S&P index temporarily lost USD 136.5 billion in value, but it quickly recovered. The Twitter accounts of BBC, CBS, France 24 TV, Al Jazeera, and National Public Radio (NPR) were also hacked. The British newspaper "The Guardian" was affected by an attack of this type on 29 April 2013. Anti-Israeli slogans and texts such as "Long Live Syria" and "The Syrian Electronic Army was here" were disseminated. The victims also included FIFA and its president Joseph Blatter. This account was used to spread the false news that Blatter was resigning from his position on accusations of corruption because he had taken money from the Emir of Qatar in return for the awarding of the 2022 World Cup.

The attacks were alleged to have been perpetrated by the "Syrian Electronic Army (SEA)", which wants to cause "chaos and embarrassment". Clearly, the SEA also wanted to raise its profile. The SEA accuses Western media of spreading "lies and defamation about Syria".

The method is always the same: Attackers send credible e-mails with a link to an infected site to the Twitter account holders. The malware installed in this way attacks user names and passwords, with which the attacker can then log on to the account and spread messages.

The influence of social media on the spread of information is steadily growing. The competition among media also means that there is less and less time to verify a news item, especially if the item appears to come from a renowned source. It can easily be forgotten that Twitter accounts are protected only by a user name and password. A targeted attack using the familiar *phishing* and *malware* methods is enough to obtain the passwords. Twitter has therefore sent a warning to the media industry stating that such attacks are likely to continue, especially against respected and popular media. To keep the risk of a malware infection low, Twitter recommends using a separate computer to send tweets, in addition to the usual measures. Twitter is also said to be considering technical measures and working on introducing *two-factor authentication* as is used by e-banking, for instance.[23]

Bogus messages via Twitter are also possible even if no account has been compromised, as the example of Andrea Caroni showed in November 2011. Although National Councillor Caroni did not have a Twitter account, a bogus account in his name confirmed the re-election of Federal Councillor Eveline Widmer-Schlumpf even before the official result was announced.[24]

Apart from all the technical measures, it should be considered and defined in advance how and via which channels a bogus message should be denied most efficiently or corrected so that even greater confusion and other consequences can be avoided.

[23] http://www.zdnet.de/88155870/twitter-fuhrt-zwei-faktor-authentifizierung-ein/?ModPagespeed=noscript (as at 31 August 2013).

[24] MELANI Semi-annual report 2011/2, Chapter 3.6: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=en (as at 31 August 2013).

4.5 SCADA systems and industrial control systems: Open access, vulnerabilities, attacks, and protection

Control systems consist of one or more devices that control, regulate, and/or monitor the behaviour of other devices or systems. In industrial production, the term "industrial control system" (ICS) is often used. Industrial control systems recently have been found more frequently beyond applications in the manufacturing industry as well, such as home automation and traffic control. In principle, an industrial control system can refer to any system regulating and/or monitoring a physical process. Most of the basic rules for protecting such systems can also be applied beyond industry.

Open serial-port server on the Internet

Serial-port servers offer a transition from a telecommunication network to serial device *interfaces*. Investigations by the security researcher HD Moore[25] have shown that of more than 100,000 such servers, relatively unimpeded access from the Internet in one form or another was possible for about 10% of them. These included various facilities – from ICS for boiler facilities in a brewery and corporate *VPN servers* to *smart metres* and traffic light controls – whose open access entails considerable potential for misuse.

Many devices that can be accessed via a serial interface do not need further authentication, since they assume in the case of a physical connection via a serial interface (which until now has always been local) that the connecting person is authorized both to access the device and change its configuration. This circumstance must be taken into account when upgrading remote access. Remote access must always be protected from misuse. For this purpose, VPN tunnels and/or restricted access to just a few known IP addresses can be used. Beyond this, attention must be paid that access is always encrypted and that only strong passwords or *two-factor authentication* are employed.

Vulnerability in control modules: Passwords readable

The micro-cogeneration unit "ecoPower 1.0" is a power and heating system with a gas combustion engine for private use manufactured by Valliant. The heater also produces electricity, which can be used by the owner or fed into the public grid. The device is controlled using a built-in touch screen, and iPad *app* or a *web interface*. When implementing remote control via the Internet, however, several security mechanisms were not designed optimally or were omitted altogether. For instance, a vulnerability allows all passwords to be tapped. In addition to the configuration password of the user, these include the passwords for remote control service and even for system developers – all of which are outputted in plain text by the system. This allowed unauthorized third parties to access the micro-power plant, read user data, and change operational settings. After the user of one of these devices reported this to security experts[26] who researched the problems, the manufacturer was briefed on the results. Consequently, the manufacturer recommended to all affected clients in writing that they un-

[25] https://community.rapid7.com/community/metasploit/blog/2013/04/23/serial-offenders-widespread-flaws-in-serial-port-servers (as at 31 August 2013).

[26] http://www.bhkw-infothek.de/nachrichten/18555/2013-04-15-kritische-sicherheitslucke-ermoglicht-fremdzugriff-auf-systemregler-des-vaillant-ecopower-1-0/; http://heise.de/-1840919 (as at 31 August 2013).

plug the network cable from the Internet until a solution had been found and a technician came to resolve the problems onsite.

Although Valliant had to face accusations that its products violated all security recommendations by being directly connected to the Internet – not via an encrypted *VPN* tunnel, it was especially Saia-Burgess, the Swiss manufacturer of the control modules, that had to deal with the problem, since it was responsible for saving the passwords in plain text and the security breach that could be used to tap the passwords. These control modules are namely not only used by Valliant for its heaters, but also in a wide range of devices, some of which are large and important.

Both Valliant and Saia-Burgess are undertaking[27] to fix the vulnerabilities, and they have published updates to this effect[28]. Valliant also has set up a hotline for affected clients and is installing updates and a *VPN* box for secure access. Considerable effort will be needed, however, before the updates and additional security measures have been implemented in all affected systems.

This case is a good example of the problem that must be taken into account in the development of an increasingly networked society (that no longer uses just a single network). Remote access to a device offers new opportunities and significant advantages both for users of the device and for technicians maintaining the device, but it also entails new attack points and corresponding risks. For this reason it is important that all companies involved in the supply chain of a project not only critically examine the user friendliness of new devices, but also make security demands so that they enter into consideration already during the development process: Security is a shared responsibility! While the manufacturer of the control module recommends that its devices not be connected directly to the Internet (very clearly and emphatically at the latest since the incident described above), this does not release it from the obligation to build its products in accordance with security specifications and where needed also to send out security updates within a useful time period.

Already before the Internet era, ICSs were sometimes connected to the telecommunications network – usually through their own phone line. Using this connection, it was generally the case that only the manufacturer/supplier could connect to the device for diagnosis and service purposes, so that an onside visit was necessary. If the Internet is now used for such access, the special characteristic of the Internet must be taken into account. The risk that someone finds out the telephone number of a device, cracks any existing password, and even understands the control protocol – which typically is proprietary – is probably lower than the risk that someone uses a specialized search engine[29] to find a device on the Internet and searches its embedded webserver for vulnerabilities using standard tools. If there is a need to administer such systems remotely, this may for instance be made possible using encrypted VPN tunnels with strong authentication.

The upset caused by the vulnerable control systems also has a positive side: The topic of security is now discussed much more actively in the industry.

[27] http://www.heise.de/newsticker/meldung/Kritisches-Sicherheitsupdate-fuer-200-000-Industriesteuerungen-1934787.html (as at 31 August 2013).

[28] Firmware Update by Saia: http://www.sbc-support.com/de/product-index/firmware-for-pcd-cosinus.html (as at 31 August 2013).

[29] See, e.g., Shodan search engine: http://www.shodanhq.com (as at 31 August 2013).

Industrial control systems (ICSs) attacked

Kyle Wilhoit, a researcher at Trendmicro, examined attacks on ICSs with the help of *honeypots* over an extended period of time. He discovered that automated and semi-automated attacks against ICSs take place on a continuous basis.

He gained the following insights in this regard:

- More than 16,000 automated attacks over a period of 5 months, which originated from 605 different *IP addresses*. He did not count attacks that had nothing to do with ICSs.

- The following attacks were discovered, among others:
  - attempted access to the diagnosis sites for the simulated systems
  - attempted access and modification of *Modbus/DNP3* traffic
  - attempts to modify the (simulated) pump system
  - attempts to access protected areas
  - unauthorized read and write attempts to *PLCs*.[30]

- Targeted attacks with malware against an e-mail address published on the honeypot were observed. In this way, the attacker tried to steal data that would be useful for further attacks (information on *VPN* configurations, network settings, and the Windows password database).

The analysis by Kyle Wilhoit shows that ICSs connected to the Internet are attacked regularly, regardless of whether they belong to a well-known and especially exposed facility or not. ICSs should therefore never be connected directly to the Internet without additional protection mechanisms.

What can be done to protect industrial control systems (ICS)?

SANS[31], a security institute in the United States, has published 20 key elements[32] on how ICT infrastructures can be protected in general. These elements may in part also be used on ICSs. Other recommendations have been published by the US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT[33]) and the National Institute of Standards and Technology (NIST[34]).

The following 11 security recommendations are based on these documents. More detailed explanations can be found on the MELANI website[35].

1. Create and maintain asset database for all devices

[30] PLC means "programmable logic controller" and is used to control a facility.

[31] SANS, http://www.sans.org (as at 31 August 2013).

[32] SANS Top 20 Critical Security Controls: http://www.sans.org/critical-security-controls/ (as at 31 August 2013).

[33] ICS CERT: http://ics-cert.us-cert.gov/ (as at 31 August 2013).

[34] NIST: http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf (as at 31 August 2013).

[35] Checklists and instructions: http://www.melani.admin.ch/dienstleistungen/00132/index.html?lang=de (as at 31 August 2013).

2. Establish life cycle and patch management for software
3. Define and use secure configurations
4. Plan and build robust network architectures
5. Implement multi-stage malware protection
6. Authentication and authorization
7. Set up central log analysis
8. Ensure physical protection
9. Carry out and regularly test backup and recovery
10. Establish and practice security incident management processes
11. Establish a security culture

It is important to understand that in most cases, security cannot be guaranteed immediately and with a one-time action, but rather must be improved in a continuous process that never ends. It is accordingly useful to define realistic, reachable goals and to work on those points first that increase security in a noticeable way with relatively little effort, e.g., changing all default passwords and protecting control interfaces that can be accessed from the outside.

While in the case of classic IT systems, confidentiality and integrity are just as important as availability, the focus in the case of ICSs tends to be more strongly on availability. But protecting confidentiality and integrity also serves to ensure availability. A system communicating via a protocol that protects the confidentiality and integrity of the transmitted data is better protected against attacks at the network level and in that way helps ensure better availability.

4.6 Software failures and their impact

Errors in the reservation system – numerous American Airlines flights cancelled

On the morning of 16 April 2013, a computer error in the booking system of American Airlines led to a breakdown. As a consequence, no airplanes could be released for several hours. Only in the afternoon were the systems back up and running. A total of 700 flights were cancelled, and even more flights were delayed. The US airline operates about 3,400 flights each day[36]. The cause of this glitch was not communicated.

This example illustrates that not only disruptions to SCADA and industrial control systems may result in breakdowns of critical infrastructures. Especially when physical processes depend on the availability of data(bases), problems of this kind may have serious consequences.

[36] http://www.handelszeitung.ch/news/peinlicher-computerfehler-american-airlines-kann-nicht-fliegen (as at 31 August 2013).

Due to a software error, Chrysler calls back hundreds of thousands of SUVs

Recalls in the auto industry are not unusual. More and more frequently, recalls are also due to faulty errors. In May 2013, for instance, Chrysler recalled more than 400,000 SUVs due to faulty software. In some vehicles, the software shifted gears unexpectedly, which in the worst case could lead to an accident.

More and more functions in modern cars are controlled by software, so it is only a question of time until software errors surface with increasing frequency in cars as well.

4.7 Operations, indictments, and arrests against cyber-criminals

There were various police operations, arrests, and convictions of cybercriminals in the first half of 2013.

DDoS: Operation Payback

In January 2013, an English court sentenced Christopher Weatherhead of the Anonymous movement to 18 months for his role in Operation Payback[37] against PayPal, MasterCard and Visa. The punishments for other Anonymous activists were less severe. The court found that Weatherhead had played a leading role in the operation.

E-banking malware: Gozi

Also in January 2013, US justice authorities filed criminal charges against three people for authoring and distributing the e-banking *malware* Gozi. Gozi is claimed to have infected more than a million computers around the world, causing millions of dollars in damage.

Ransomware: Reveton

In February 2013, the Spanish police arrested several authors and operators of the *ransomware* Reveton, including the alleged head of the criminal group. The malware Reveton blocks an infected computer and displays a supposed message from the police on the monitor accusing the victim of several criminal acts. The message says that if a certain sum of money is paid, prosecution will be waved and the computer unblocked. The ransomware was adapted specifically to different countries and has infected numerous computers in nearly thirty countries, including in Switzerland; see the MELANI Semi-annual report 2012/I[38]. The arrests were made thanks to cooperation between the Spanish police, Europol, Interpol, and the Internet security firm Trend Micro. Reveton and its variants continue to be active after the arrests, however, including in Switzerland.

[37] MELANI Semi-annual report 2010/2, Chapter 3.2: http://www.melani.admin.ch/dokumentation/00123/00124/01122/index.html?lang=en (as at 31 August 2013).

[38] MELANI Semi-annual report 2012/1, Chapter 3.3: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=en (as at 31 August 2013).

Botnet: Citadel

In a joint action disclosed on 6 June 2013, the American Federal Bureau of Investigation (FBI) and the software company Microsoft deactivated nearly 1,400 servers used by Citadel. This widespread *malware* has existed since 2011 and is used to commit e-banking fraud, also in Switzerland. According to Microsoft, Citadel is responsible for losses in the amount of USD 500 million from clients in numerous financial institutions. Citadel is a personalizable e-banking malware available on the Internet underground market and is used by numerous criminal groups.

The FBI and Microsoft carried out the operation called b54 in cooperation with financial institutions and law enforcement authorities in several countries. The deactivated *command and control servers* were used to control and administer botnets. In this connection, the FBI are looking for a person who calls himself or herself Aquabox and is suspected of being the author of the software.

Operation "b54" will no doubt disrupt the good business of the various criminal groups using Citadel. However, it is not likely that this operation will have a sustained impact. Similarly, it is not likely that the existence of the malware is in danger. The ability of malware and botnets to regenerate after such operations has already been proven in the past. New functions may even be added, making it even more difficult to detect the malware used and render it harmless.

4.8 Fourth international Cyberstorm exercise

On 20 and 21 March 2013, the fourth international Cyberstorm exercise took place. In these exercises, the member countries of the International Watch and Warning Networks (IWWN), including Switzerland, test their cooperation and ability to respond to a cyber attack. This year's exercise primarily aimed to test standard procedures to facilitate the handling of a cyber incident.

Cyberstorm is an international cyber exercise initiated by the United States and specifically by the Department of Homeland Security to test the ability to respond to cyber incidents. The exercise is mainly tailored to the US and its security organizations, but it has also had an international component since its first year. The first exercise of this type took place in 2006. Analogously to the European exercise Cyber Europe 2012, standard operating procedures (SOPs) were tested for their effectiveness in Cyberstorm IV. These SOPs govern the establishment of contact, information exchange, and cooperation in the event of an international cyber incident.

This year's exercise scenario assumed the infection of major media portals and administration computers as well as a data outflow to foreign servers. The complexity of the exercise, which lasted more than 32 hours, made it possible to test cooperation between the participations. In total, 300 events were simulated.

Incidents in cyberspace are almost always cross-border. A joint international approach is therefore necessary to deal efficiently with cyber crises. The exercise showed that information exchange functions smoothly and efficiently between the countries at the technical and operational level. A special challenge, however, is the evaluation of the large volume of available data, so that a situation analysis with all relevant information can be prepared as a basis for decision-makers in a real emergency.

5 Trends/Outlook

5.1 On states, the economy, and the law

Every company, whether it operates only in its home market or globally, is subject to the legislation of the country where it is active. The place where the headquarters are located plays an important role in this regard. This is where the general management, typically the highest decision-making body, is located and – depending on the field of business – probably also the main location for production, logistics, and administration as well the information relevant to business operations.

This basic iron rule is true of both machine manufacturers and fast food chains as well as major companies whose products and services supply the foundation and basic infrastructure of worldwide networks. It goes without saying that the nationally applicable laws also include security laws which, in the context of criminal prosecutions or suspicions of terrorist activities, are able to lift data protection in certain cases. The fact that highly specialized technology companies must disclosure certain foreign operations to the national control authority, in order to prevent exports of dual-use goods to countries that do not respect basic human rights, is generally accepted. The main problem has less to do with the sense and purpose of these laws, but rather with their impact and application.

In the case of providers of information and communication technologies, this logic is complicated by an additional element: The overwhelming majority of providers of information and communication technologies – whether software and hardware manufacturers, *cloud* providers, or data transmission services – are headquartered in the United States and so they are primarily subject to American legislation and jurisprudence. Centralization of market power for a given sector in a single country also leads to a concentration of possibilities by the government of that country to use its legislation to access the core infrastructure providers of worldwide networks. It appears clear that in such cases, application of national laws also always has a global impact. From this perspective, the United States enjoys a de facto unipolar, hegemonic position in the world with regard to ICT companies and their role as drivers and maintainers of global networks. It might be argued that China likewise enjoys overwhelming market power in the manufacture of hardware components – catchword: supply chain. This issue will certain be in need of significant clarification in future. But final operation of this hardware outside China, development of the firmware that control these components, etc., is often not in Chinese hands. Especially in regard to search engines, e-mail systems, and social media, China is pursuing local solutions that do not have global implications and do not compete in this sector with the dominance of the companies located in the United States.

In the past, the hegemonic position of certain countries also always entailed a whole set of sensitive security-policy questions for other countries, their economies, and their populations. Always associated with this set of issues is the question of the extent to which the hegemon is willing to assert its dominance against others, and whether the hegemon is even aware of its dominance and the global implications arising from that dominance. In the end, these questions relate to the hegemon's predictability in terms of protection from arbitrariness and abuse of power, which constitutes an important factor for other states' dealings with hegemon. And ultimately, this predictability (in terms of planning and legal certainty) also form the foundation for the business sector's dealing with necessary partners within the legal sphere of influence of the hegemon.

It should be in the interest of every state with such a dominant position to clarify precisely these questions early on and conclusively. This is not a question of legal sovereignty, but rather primarily of (political) clarification regarding the goals the hegemon's legislation pursues and to what extent the hegemon intends to issue and apply legislation for the benefit of its own (particular) interests at the expense of foreign interests – i.e., to what extent the hegemon is willing to use its legal order and accordingly its influence on domestic (but possibly globally operating) industry to pursue its own security policy (and possibly economic) interests to the disadvantage of other states, or to what extent it expressly refrains from doing so. But it is also the responsibility of the international community to raise these questions in an international discourse and to work toward clarification in one direction or the other. Switzerland in particular is active in these areas in multilateral and bilateral forums.

A long-lasting phase of uncertainty and unpredictability would undoubtedly mean that states would have to use their own independent ICT solutions – not as part of a sporting competition guided by the rules of the market economy, but rather as a security policy instrument and a way to establish boundaries in relation to the products from the hegemon's country. It goes without saying that this is associated with inefficiency and disproportionate costs for the business sector and especially the critical infrastructure as well, and it should therefore always be considered the worse solution.

For many years, the Reporting and Analysis Centre for Information Assurance (MELANI) has advocated a risk-based approach to information assurance and the protection of ICT infrastructures, and it has now been included in the Federal Council's National Strategy for the Protection of Switzerland against Cyber Risks (NCS). This is instead of a purely technical approach on the basis of ICT possibilities. Alternatives in the domain of router products and market-economic programmes induced in this domain outside the United States and China already exist today and are also employed accordingly.[39]

For this approach to cyber risks to succeed, it is essential that the threat be assessed and understood in its many different manifestations. Not only actors, technical vulnerabilities, and the most recent insights on incidents play a role in this regard, but also non-technical factors relating to physical, personnel, and organizational design, legal framework conditions, and sovereign interventions in the country of the product manufacturers, service providers, and data storage systems employed. It should be up to each company to weight those risk factors more or less heavily that correspond most closely to its profile, its critical processes and exposure abroad, and its business activities.

In order to offer greater support in this area to businesses and especially to critical infrastructures in future, the National Strategy for the Protection of Switzerland against Cyber Risks (National Cyber Strategy, NCS) is committed to increasing MELANI staff by 2017 and

[39] http://www.fp7-ofelia.eu/about-ofelia/ (as at 31 August 2013).
http://www.change-project.eu (as at 31 August 2013).
http://www.openflow.org/wk/index.php/MPLS_with_OpenFlow/SDN (as at 31 August 2013).
http://www.heise.de/ix/artikel/Alles-fliesst-1643457.html (as at 31 August 2013).

strengthening the resources that enhance Switzerland's position and that of its business sector in the domain of international security policy.

5.2 Tallinn Manual

In March 2013, the Tallinn Manual (Tallinn Manual on the International Law Applicable to Cyber Warfare) was published.[40] This is a study on how international law – especially the "right to war" (jus ad bellum) and international humanitarian law ("law of war", jus in bello) – might be applied to cyber operations.

In 95 commented rules, the Tallinn Manual deals with questions including state sovereignty, jurisdiction, responsibilities, and implications for neutrality law. It discusses when a civilian hacker can be deemed an active combatant and accordingly becomes a legitimate military target, or to what extent these activities can be attributed to a state. The protection of critical civilian infrastructure and attacks on nuclear power plants and dams are also discussed[41].

The Manual was prepared between 2009 and 2012 by an international group of approximately 20 experts in different domains at the invitation of the NATO Cooperative Cyber Defence Center of Excellence headquartered in the Estonian capital of Tallinn. It is not an official NATO document, but rather a legally non-binding academic publication showing approaches and (sometimes divergent) opinions on how existing international law can be applied to the new cyber environment. Since it is the first detailed publication in this field, it should be assumed that despite its non-official character, various states and organizations will observe the presented opinions when formulating their own positions and guidelines.

5.3 End of support in sight for Microsoft Windows XP SP3 and Microsoft Office 2003

On 8 April 2014, support for Microsoft Windows XP SP3 and Microsoft Office 2003 will come to an end. All companies working with these versions are urgently recommended to upgrade to newer operating system and software versions that continue to be supported.

After 8 April 2014, neither support nor security *patches* and problem solving will be freely available from the manufacture for Windows XP SP3 and Office 2003. Vulnerabilities of operating systems and applications no longer supported will not be fixed, a fact that can be exploited for targeted cyber attacks against computers continuing to use Windows XP SP 3 and/or Office 2003. The chance of success of such attacks is higher, and accordingly the security risk for users employing the old versions also increases.

The most recent software versions offer improvements in terms of security, since they contain the most up-to-date security technologies. Additionally, the manufacturer will continue to eliminate vulnerabilities that become known. In addition to *patch* management, using the most recent operating systems and applications is one of the most effective ways to improve security.

[40] http://issuu.com/nato_ccd_coe/docs/tallinnmanual?e=5903855/1802381 (as at 31 August 2013).

[41] http://ccdcoe.org/249.html (as at 31 August 2013).

For companies that are unable to perform the upgrade by 8 April 2014, there is the option of concluding a service support agreement with Microsoft. The costs for service support are considerably higher than for normal support, and they rise over time. Companies choosing the service support must, as part of the agreement with Microsoft, also present a plan for their transition from Windows XP SP3 and Office 2003 to newer products.

Support for Microsoft Exchange Server 2003 and Microsoft Office SharePoint Server 2003 will likewise end on 8 April 2014.[42]

5.4 Content management system (CMS) as a problem zone

The number of websites has truly exploded over the past few years. This is in part because even users without technical expertise can often place their own website on the Internet with easy-to-use tools and at lower and lower costs. Content management systems (CMSs) are often used for this purpose, with which a website can be designed and placed online with only a few clicks and without detailed knowledge in web design. There are now dozens of such CMSs used by hobby website operators, SMEs, and others. The increasing popularity of these systems makes them interesting for cybercriminals as well, who invest all the more energy and effort in their search for vulnerabilities the more popular a software program is and accordingly the greater the number of potential targets. Not only CMSs, but every software program has potential vulnerabilities – no program is guaranteed to be secure. Moreover, software developers implement new functions all the time. But with each additional line of code, the software not only gets more functions, but its complexity also increases and accordingly the risk that it might have a vulnerability somewhere.

Vulnerabilities are not usually hidden from software developers for very long, and often it takes only a few days from the discovery of a vulnerability until a software update is supplied by the manufacturer that is intended to fix it. Since these software updates are not automatically installed on the system, the website operator must act. Because many websites are now being operated by technical laypersons, who are given simple tools for setting up a website but not the necessary explanations enabling them to maintain it in a secure way, there are accordingly many websites using CMSs that have not been updated for months or even years and may already contain dozens of (known) vulnerabilities.

Such vulnerable websites can be found and attacked automatically using appropriate tools. It is relatively easy for criminals to manipulate a large number of websites in this way so that their visitors are infected with malware.

Attacks on CMSs can be reduced dramatically by way of *patching* (prompt incorporation of security updates). However, several other measures can contribute to the security of CMSs.

[42] Detailed information on the MS Support Lifecycle: http://support.microsoft.com/lifecycle (as at 31 August 2013).
Detailed information on the end of support for Windows XP SP3 und Office 2003: http://www.microsoft.com/endofsupport (as at 31 August 2013).

Explanations of the enumerated measures can be found on the MELANI website under "Checklists and instructions"[43].

1. Prompt incorporation of security updates
2. Two-factor authentication
3. Restriction of administrator access to certain IP addresses
4. Restriction of administrator access using a .htaccess file
5. Securing the computer of the webmaster
6. Web application firewall
7. Early recognition of vulnerabilities.

5.5 Where people meet (and infect each other) – the watering hole

In dry regions, all animals eventually come to the watering hole to drink. This phenomenon lends its name to a type of attack that has become more common recently: the *watering hole attack*. Also on the Internet, there are places where Internet users regularly hang out – not to gather water or food, but information. While search engines, news portals, and social networks attract a large number of very different kinds of persons, there are websites of thematically specialized information providers that are regularly visited by users interested in the information they offer. This can be exploited by an attacker targeting specific professional or interest groups. If the attacker is able to hack a website and place *malware* on it, the attacker gains access to a targeted public.

In spring 2013, for instance, the website of the US Department of Labor was hacked and a *drive-by* infection was placed on it, which exploited a previously unknown *vulnerability* in Internet Explorer 8. On the site in question, employees of energy companies can obtain information on compensation programmes after coming into contact with uranium. The computers of the interested users accessing this site were infected with espionage software. This targeted placement lends itself to the conclusion that the attackers were targeting individuals working in the energy sector – especially nuclear power plants – and government employees in this field. But also persons working with nuclear weapons were in the focus of the attackers.

Reports of such watering hole attacks increased during the reporting period. Unlike conventional drive-by infections, in which criminals exploit poorly protected websites without discrimination in order to spread their malware on arbitrary computers, watering hole attacks require considerably more effort to hack specific websites without regard to the available security measures.

Although these attacks primarily target office computers, other sensitive information (network plans, addresses and access data for control systems, etc.) in addition to trade secrets may be obtained depending on the company in question, and this information can then be used

[43] Checklists and instructions: http://www.melani.admin.ch/dienstleistungen/00132/index.html?lang=en (as at 31 August 2013).

for various additional attacks. In an insufficiently segmented corporate network, the hackers can also jump from system to system until they finally reach a system that controls physical processes, in order to manipulate such a control system.

Sooner or later, a *vulnerability* will surface in every browser. In Chapter 5.1 of the MELANI Semi-annual reports 2012/2[44], we presented possibilities for minimizing risk when browser vulnerabilities become known. However, there is always the possibility that watering hole attacks are carried out with vulnerabilities that are still unknown at the time (also in *plug-ins*).

5.6 Smartphone trojans

The trend of malware on smartphones again continued in the last half year, increasing strongly over the past few months. The focus is mainly on the Android operating systems. The reasons can be found in the great popularity of Android, its open structure as already discussed in the last semi-annual report[45], but also in the fact that a large number of manufacturers do not supply security updates until long after a vulnerability becomes known, if at all.

The attackers' goals vary considerably:

- Attacks on bank accounts: theft of *mTANs*
- Sending of premium SMSs
- Attacks against mobile micropayment applications
- Theft of access data for social networks and e-mail accounts
- Address data: names, telephone numbers, e-mail address, and birthdates of contacts
- Identity theft
- General data theft.

Very often, a social engineering component for spreading malware is employed. For instance, known apps are trojanized and circulated using a non-official app store. E-mails are sent in advance with the infected links, such as bogus e-mails from a bank providing information about a new app that has to be downloaded to use online banking. *Drive-by infections* have also been observed where it suffices in principle for the user to visit a website in order for the device to become infected. A new dimension is achieved with the appearance of the first botnets that consist only of Android devices. These are, for instance, used to send spam e-mails.

Interestingly, a large proportion of the *malware* being circulated in this way are built on the same basic code. For instance, a certain library (libvadgo) has been found in various malware variants, serving to communicate with *command-and-control servers*. This library can

[44] MELANI Semi-annual report 2012/2, Chapter 5.1: http://www.melani.admin.ch/dokumentation/00123/00124/01535/index.html?lang=en (as at 31 August 2013).

[45] MELANI Semi-annual report 2012/2, Chapter 4.8: http://www.melani.admin.ch/dokumentation/00123/00124/01535/index.html?lang=en (as at 31 August 2013).

also conceal itself from analysis tools by ending certain processes or manipulating certain commands.

Most malware for mobile devices is currently being written for Android. But also the other platforms can be attacked. Where there are targeted attacks against particular companies or groups of persons, an iPhone or Windows phone offers a similar point of attack as an Android device. Mobile devices – especially in environments that are otherwise well secured – can serve as a gateway to penetrate internal networks. This problem must be observed especially in the case of *bring your own device (BYOD)* projects.

MELANI recommends the following code of conduct for the secure use of mobile devices:

1. Properly employ the available security mechanisms on your smartphone (e.g., PIN entry and automatic locking of the home screen).
2. Only install applications from official app stores. Compare reviews and user feedback. Never install applications via links in e-mails.
3. Before installation, check the privileges required by an application and consider whether these are really necessary or whether you really want to grant them (e.g., access to the address book, or reading and sending of SMSs). When in doubt, do not install.
4. Exercise caution when using unknown WiFi hotspots. Configure your smartphone so that it does not automatically join new wireless networks.
5. For Android devices version 4.2 and higher: Ensure Google's reputation service is active; this protects your device from known threats (malicious apps). The app can be configured in the "Google settings" app in the menu point "Verify apps". The "Verify apps" box should be checked.
6. For Android devices: Make sure that the installation of apps only from the official Google Play Store is permitted (the "Unknown sources" option under Settings -> Security -> Device administration should be deactivated).

Annex 7.1 contains an analysis of the Android trojans surfacing in Switzerland in the first half of 2013.

5.7 Fraudulent use of and attacks against Internet telephony (VoIP)

The risks in the use of VoIP technologies and the possibilities of fraudulent use affect both private individuals and businesses. The damage potential of a misuse of VoIP infrastructure is much greater for businesses, however. Finally, the undisputed economic advantages of VoIP telephony must always be weighed against the possible disadvantages in terms of security. Fraud perpetrated in whole or in part by phone now largely makes use of VoIP technology. An example from Switzerland is described in Chapter 3.6. Other possible types of attacks are described below:

Telephony denial of service

At the beginning of 2013, American authorities drew attention to the threat of *telephony denial of service*, i.e., attacks against the availability of telephone services. For this purpose, a telephone exchange is flooded with calls so that it can no longer be reached. These attacks are automated by a (compromised) VoIP device and carried out without great costs. Usually, such an attack is accompanied by a demand for money. The operators of the line are asked to pay a certain sum for the attack to cease. The phenomenon is particularly worrisome if it affects public services and especially medical emergency numbers.

Espionage

VoIP converts conversations into digital data. Analogously to all other digital data, attackers may try to obtain this data as well. There are various tapping methods: Some malware is conceived so that it is installed directly on a computer and gathers the signals of conversations from there before they are encrypted and sent via *IP protocol*. Other attacks occur directly on VoIP servers in order to spy out the communications routed through them. It should also be noted that the transfer of stolen data is in some cases concealed as VoIP traffic.

1. A first basic rule to minimize the risks of using this technology is – as simple as it sounds – changing the initial access codes into complex passwords.

2. As is the case for all other software products, the programs used for VoIP must be updated on a permanent basis.

3. One specific security measure is to configure VoIP telephones in such a way that only calls to specific number ranges are possible and that calls to premium numbers are blocked where possible.

6 Glossary

Advanced Persistent Threats (APT)	This threat results in very great damage impacting a single organisation or a country. The attacker is willing to invest a large amount of time, money and knowledge in the attack and generally has substantial resources.
App	"App" (an abbreviation of "application") generally refers to any type of application programme. In common parlance, the term now generally refers to applications for modern smartphones and tablet computers.
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.
Bring your own device (BYOD)	Bring your own device (BYOD) is an organizational guideline governing the ways in which employees can use their own electronic office devices for business purposes.
Brute force	The brute force method is a solution method for problems in the field of computer science, cryptology, and game theory that relies on trying out all (or at least many) possible cases.
Cloud Computing	Cloud computing (synonym: cloud IT) is a term used in information technology (IT). The IT landscape is no longer operated/provided by the provider himself, but rather obtained via one or more providers. The applications and data are no longer located on a local computer or corporate computing centres, but rather in a cloud. These remote systems are accessed via a network.
Command & control server	Most bots can be monitored by a botmaster and receive commands via a communication channel. This channel is called command & control server.
Content Management System	A content management system (CMS) is a system that makes possible and organizes the joint preparation and processing of content, consisting of text and multimedia documents, generally for the World Wide Web. An author may operate such a system even without programming or HTML knowledge. The information to be displayed is referred to as "content".

Data packet	A data packet in data processing is very generally speaking one of the terms referring to self-contained data units that a sender or a sending process sends to a recipient.
Distributed Denial Of Service (DDoS)	Have the goal of causing a loss of a specific service to users or at least to considerably restrict the accessibility of the service.
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).
DNS amplification attack	A denial of service attack (DoS) that exploits publicly accessible DNS servers and uses these as amplifiers.
DNS reflection attack	See DNS amplification attack.
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.
Firewall	A firewall protects computer systems by monitoring incoming and outgoing connections and rejecting them if necessary. A personal firewall (also called a desktop firewall), on the other hand, is designed to protect a stand-alone computer and is installed directly on it.
Flash	Adobe Flash (or simply "Flash", formerly "Macromedia Flash") is a proprietary, integrated development environment for creating multimedia content. Flash is now used on many websites, whether as web banners, as part of a website (e.g. as a control menu) or in the form of entire Flash pages.
FTP	FTP is a network protocol for transferring data via TCP/IP networks. FTP can be used, for instance, to load websites onto a webserver.
Gateways	A gateway connects computer networks that can be based on completely different network protocols.
Geolocation	Geolocation assigns IP addresses to their geographic origin.

Honeypots	In the field of computer security, a honeypot is a computer programme or server that simulates the network services of a computer, an entire computer network, or the behaviour of a user. Honeypots are employed to obtain information on attack patterns and attacker behaviour.
Hyperlink	A hyperlink, or link for short, is an electronic cross-reference in a hypertext that functionally performs a jump to a different location within the same document or to a different electronic document.
Interface	An interface is the part of a system serving communication. See web interface.
Internet Protocol (IP)	The Internet Protocol (IP) is a widespread network protocol in computer networks, constituting the basis of the Internet. It is the implementation of the network layer of the TCP/IP or OSI model.
Internet Service Provider (ISPs)	Companies that provide different services, mostly against payment, which are necessary for using or operating internet services.
Intrusion Detection Systeme	System with which unauthorised access to data or computers can be detected.
IP address spoofing	In information technology, "spoofing" refers to various deception attempts in computer networks to conceal one's own identity.
IP-Address	Address to uniquely identify computers on the Internet or on a TCP/IP-network (e.g.: 172.16.54.87).
Java	Java is an object-oriented programming language and a registered trademark of Sun Microsystems (bought by Oracle in 2010).
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.
Mobile banking	Mobile banking designates the transaction of banking business with the help of mobile end-user devices such as mobile telephones and PDAs.
Modbus/DNP3	Modbus and DNP3 (Distributed Network Protocol) are communication protocols for process automation systems.
mTAN	One-time password sent via SMS and used pre-

	dominantly in online banking.
Open DNS resolvers	DNS servers reachable and useable for all users on the Internet.
Open Source	Open source is a range of licences for software whose source code is publically available. Further developments are encouraged by the licence.
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.
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.
PHP-Script	PHP is a scripting language mainly used to create dynamic websites or web applications.
PLC	A programmable logic controller (PLC) is a device employed to control or regulate a machine or device, programmed on a digital basis.
Plug-Ins	(Additional) software that extends the basic functions of an application, e.g. Acrobat plug-ins for internet browsers allow direct display of PDF documents.
Point of Sales	POS terminal (in Switzerland: EFT/POS terminal) is an online terminal for cashless payments at points of sale.
QR code	A QR code is a two-dimensional barcode consisting of a square matrix made up of black and white points that display the binary encoded 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.

Remote Administration Tool	A remote administration tool is used for the remote administration of any number of computers or computing systems.
Remote Administration Tool (RAT)	A remote administration tool is used for the remote administration of any number of computers or computing systems.
Security holes	A loophole or bug in hardware or software through which attackers can access a system.
Serial-port server	A serial-port server is a device that transfers data between a serial interface and the Ethernet.
sFTP	sFTP is a model for encrypting the File Transfer Protocol (FTP) described in RFC 4217.
Smart-Meter	A smart meter is an energy meter that displays the actual energy use and actual usage period to an energy consumer; the information can also be transmitted to the energy supplier
SMS	Short Message Service Service to send text messages (160 characters maximum) to mobile phone users.
Spam	Spam refers to unsolicited and automatically sent mass advertising, into which category spam e-mails also fall. The person responsible for these messages is known as a spammer, whereas the actual sending itself is known as spamming.
Spam score	Point system used by filters to recognize e-mails as spam.
Spear-Phishing	Targeted phishing attacks. The victim is made to believe that he/she is communicating via e-mail with a person they are acquainted with.
Telephony denial of service	Attack on the availability of telephone systems, primarily for VoIP.
Two-factor authentication	For this at least two of the following three authentication factors are required: 1. Something you know (e.g. password, PIN, etc.) 2. Something you have (e.g. a certificate, token, list of codes, etc.) 3. Something you are (e.g. finger print, retina scan, voice recognition, etc.)
Virus	A self-replicating computer program with harmful functions that attaches itself to a host program or host file in order to spread.

Voice-Phishing	Voice phishing is a form of Internet scam, derived from the word "fishing" and the method of VoIP telephony used.
VoIP	Voice over IP. Telephony via internet protocol (IP). Frequently used protocols: H.323 and SIP.
VoIP toll fraud	Misuse of a VoIP device in order to call premium numbers belonging to the attacker.
VPN	Virtual Private Network Provides safe communication between computers in a public network (e.g. the internet) by encrypting the data flow.
Watering hole attacks	Targeted infection with malware using websites preferentially used only by a specific user group.
Web application firewall (WAF)	A web application firewall (WAF) is a procedure to protect web applications from attacks via the Hypertext Transfer Protocol (HTTP).
Web hosting	Web hosting, or also net hosting, refers to the provision of webspace and hosting of websites on a web server of an Internet service provider.
Web interface	The web interface is the part of a system that administers communication between the application and user, usually graphically.
Web server	A web server is a server that transfers documents to clients such as web browsers.
Zero-Day-Exploit	An exploit which appears on the same day as the security holes are made public.
zip	zip is an algorithm and file format for data compression, in order to reduce the storage space needed for the archiving and transfer of files.

7 Annex

7.1 Analysis of Android malware targeting Swiss e-banking

The functions

- The malware forwards SMSs to a mobile number in a Russian-speaking country.
- The goal is to steal mTANs.
- Upon installation, it requests the authorization to read and send SMSs as well as writing privileges for the SD card.
- It conceals itself as a certificate application of Metaforic.
- The malware is meanwhile recognized by quite a large number of virus scanners (Android/TrojanSMS.Agent.NV).

The infection

The infection occurs in the following steps:

1. The client is requested by a website to install an application for the mobile device. The client has to select the appropriate operating system.
2. A QR code is displayed that redirects to the page with the effective malware. The malware is a normal installation package for Android applications (an APK file).
3. The client must have turned off certain security settings for the installation to work.
4. As soon as the installation is executed, the malware becomes active and monitors the arrival of SMSs. The application conceals itself as a security application.
5. The SMSs are forwarded to a mobile telephone number in Russia.

The goal of the attacker is to intercept mTANs and use them for attacks against e-banking accounts.

The malware

After installation, the malware presents itself as a security application by Metaforic. Metaforic is in fact a security service provider specializing in mobile devices. A trick observed not only in the case of mobile malware is that the malicious code purports to be a trustworthy product in the security field in order to gain the victim's trust. The poor translation is striking. The user must choose a password ("Wort Dordine") and confirm it:

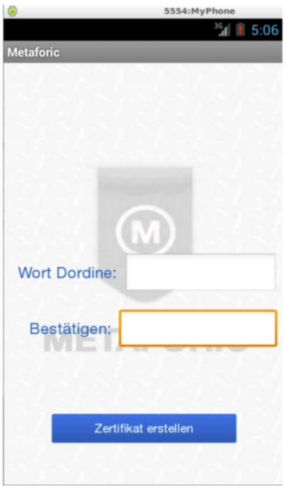
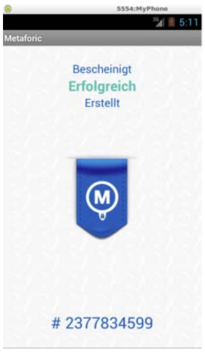


Figure 7: Displayed login screen with password entry (="Wort Dordine").

After installation of the malware, the application pretends to have successfully created a certificate.

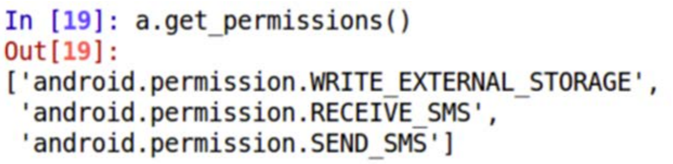


Bescheinigt
Erfolgreich
Erstellt

2377834599

Figure 8: Confirmation of the certificate installation.

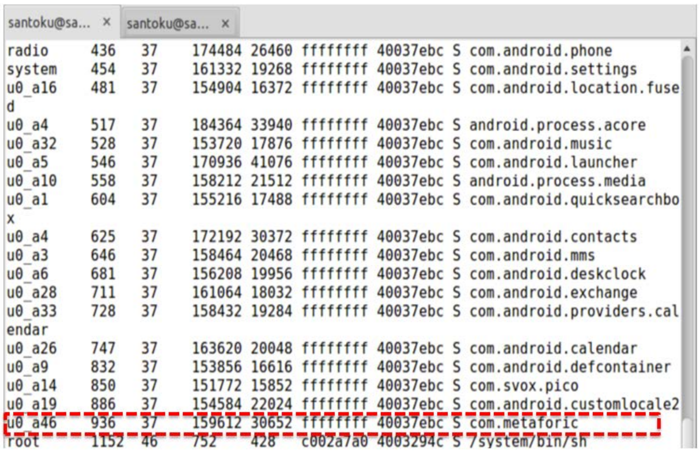
On the smartphone, the malware requests the following permissions:



```
In [19]: a.get_permissions()
Out[19]:
['android.permission.WRITE_EXTERNAL_STORAGE',
 'android.permission.RECEIVE_SMS',
 'android.permission.SEND_SMS']
```

Figure 9: Permissions granted to the malware

Especially the fact that an application requests permissions to read and send SMSs indicates that its intentions are bad. In the background, the application runs with the following process:



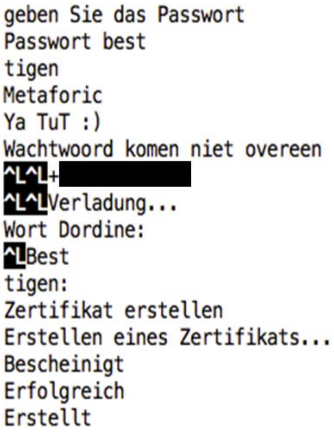
```
radio      436   37    174484 26460 ffffffff 40037ebc S com.android.phone
system     454   37    161332 19268 ffffffff 40037ebc S com.android.settings
u0_a16     481   37    154904 16372 ffffffff 40037ebc S com.android.location.fuse
d
u0_a4      517   37    184364 33940 ffffffff 40037ebc S android.process.acore
u0_a32     528   37    153720 17876 ffffffff 40037ebc S com.android.music
u0_a5      546   37    170936 41076 ffffffff 40037ebc S com.android.launcher
u0_a10     558   37    158212 21512 ffffffff 40037ebc S android.process.media
u0_a1      604   37    155216 17488 ffffffff 40037ebc S com.android.quicksearchbo
x
u0_a4      625   37    172192 30372 ffffffff 40037ebc S com.android.contacts
u0_a3      646   37    158464 20468 ffffffff 40037ebc S com.android.mms
u0_a6      681   37    156208 19956 ffffffff 40037ebc S com.android.deskclock
u0_a28     711   37    161064 18032 ffffffff 40037ebc S com.android.exchange
u0_a33     728   37    158432 19284 ffffffff 40037ebc S com.android.providers.cal
endar
u0_a26     747   37    163620 20048 ffffffff 40037ebc S com.android.calendar
u0_a9      832   37    153856 16616 ffffffff 40037ebc S com.android.defcontainer
u0_a14     850   37    151772 15852 ffffffff 40037ebc S com.svox.pico
u0_a19     886   37    154584 22024 ffffffff 40037ebc S com.android.customlocale2
u0_a46     936   37    159612 30652 ffffffff 40037ebc S com.metaforic
root       1152  46    752    428   c002a7a0 4003294c S /system/bin/sh
```

Figure 10: The malware process running in the background is marked in red.

The program code lends itself to the following conclusions:

- The application was originally written in Dutch and subsequently translated (rather badly) into German.

- The number to which the stolen SMSs are transmitted is included in plain text in the malware. The number can be localized in a Russian-speaking country.



```
geben Sie das Passwort
Passwort best
tigen
Metaforic
Ya TuT :)
Wachtwoord komen niet overeen
^L^L+[redacted]
^L^LVerladung...
Wort Dordine:
^LBest
tigen:
Zertifikat erstellen
Erstellen eines Zertifikats...
Bescheinigt
Erfolgreich
Erstellt
```

Figure 11: Source text with telephone number programmed into the code, to which the intercepted SMS is to be forwarded.

Android applications are always digitally signed. In this case, the application was signed with a debug certificate, which does not permit circulation via the official app store and the use of which is actually reserved exclusively for the development and testing of Android applications.

In general, the malware is designed very simply and neither has root kit functionality to conceal itself nor does it contain encryption or obfuscation to make analysis more difficult. It serves solely the purpose of stealing mTANs. There are many comparable trojans for the Android platform. The detection rate for the malware of the various virus scanners was initially very poor, but it subsequently rose to about 50% (as at the beginning of July 2013).