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 2016/II (July – December)

20 APRIL 2017
REPORTING AND ANALYSIS CENTRE FOR INFORMATION ASSURANCE MELANI
https://www.melani.admin.ch

1 Overview/content

2 Editorial

As Head of Group Security since September 2015, Philippe Vuilleumier is responsible for logical and physical security at Swisscom

Dear reader,

In the old days, security managers asked themselves, "What do I have to do to prevent the success of attacks against my organisation?" Today, the somewhat disillusioned question tends to be, "How long will it take until an attack is successful?" In light of the steady professionalisation of attackers, the increase in technological possibilities and the associated perfection of many attacks, it in fact makes more sense to assume that one's environment has already been compromised or will be in the near future.

Accepting this fact is one thing – drawing the right conclusions and taking the right measures is something else entirely. "Assume breach" sounds revolutionary to many at first, but what then? What can an organisation as a whole and a security team as its front line do?

At Swisscom, we have concluded that we have to do three things:

1. Continue to take our basic security seriously! This means keeping our inventories on infrastructure, data and employees current, installing the necessary updates for our systems and applications frequently, managing our risks consistently and paying attention to efficiency when undertaking all these activities.

2. Build simple security solutions! Simple for the end user. The security team makes a great contribution to the required agility in an enterprise by making technical solutions as simple and transparent as possible.

3. Emphasise detection and response! Of course prevention continues to be very important (it is part of basic security), but prevention reaches its limits at some point due to the steadily changing attack landscape. Being able to quickly detect, isolate and combat attacks and compromising incidents are important skills that we aim to improve continuously. I am pleased to mention that MELANI is an important and competent partner for Swisscom in these efforts.

The internet of things is a key topic in this report. Also in that context and given the associated challenges, the three priorities of basic security, simplicity and detection make sense.

I hope this makes for interesting reading.

Philippe Vuilleumier

3 Key topic: internet of things

Everything that can be connected will in fact be connected to the internet in the future. While this statement might be a bit of an exaggeration, it does indicate how the internet will develop in the coming years. Alongside all the conveniences arising from that development, there will certainly also be many debates about security. More and more everyday objects will be connected to the internet in the future. The first manufacturers are thus already talking about an "internet of everything" (IoE), connecting humans, processes, devices and data into an all-encompassing network. The much-cited refrigerator that automatically orders milk is a vivid example. But it is only one of many. Especially in the fields of facility management and light control, a boom has erupted in recent years.

The internet of things will be much more in the future than it is today. According to the analysts at Gartner,[1] more than 6 billion "things" were already connected to the internet in 2016. By 2020, an increase to more than 20 billion things is expected. And the possibilities of things connected to the internet are not even close to being exhausted. The internet of things will become more and more integrated into our daily life and influence it as well. Certain developments are already on the horizon: While "wearables" – i.e. applications that are worn on the body of the user or sewn into clothes, supplying a large volume of data – are still in their infancy, they will go far beyond the already established fitness trackers. Also in medicine, a multitude of applications should be expected, facilitating permanent and improved diagnostics. It is conceivable that the status of all vital organs might be accessed on a smartphone at any time. Another key area will be self-driving cars. First attempts have already been made. But to guarantee smooth and secure functioning, numerous sensors in and around the car are necessary. Independently of the development of such vehicles, numerous sensors will be built along roads to master the steadily increasing flow of traffic. Capturing data is the key topic here: self-sufficient and autonomously operating sensors transmitting their data via the internet are to help make decisions, trigger actions and, in that context, recognise dangers early on in order to avert them.

3.1 Definition

The term "internet of things" refers to the increasing networking of everyday objects and devices via the internet. The term surfaced for the first time at the end of the 1990s and was used by technology pioneer Kevin Ashton as an important basis for exchanging data between two intelligent devices.[2] There is still no uniform definition, however. The term can also be understood broadly as a synonym for connecting the real world with the virtual world.[3] One concrete implementation is the identification of tangible objects using RFID chips, QR codes and barcodes. A scanner is used to connect to the internet. This turns a simple object into an intelligent object, i.e. an object enriched with information and services. In manufacturing, the term "Industry 4.0" is often used to describe the use of intelligent objects and sensors, referring to the fourth industrial revolution brought about by digitalisation.

[1] http://www.gartner.com/newsroom/id/3598917 (as at 28 February 2017)

[2] http://www.rfidjournal.com/articles/view?4986 (as at 28 February 2017)

[3] http://www.computerwoche.de/a/industrie-4-0-ist-das-internet-der-ingenieure,2538117 (as at 28 February 2017)

3.2 The unsecure internet of things?

With the increasing possibilities of the internet (of things), we will also have to deal increasingly with the risks and side effects. For instance, care should always be taken that the refrigerator orders the milk, and not the other way around. Fundamental questions will arise that not only concern maintenance and security standards, but especially also data protection. The purpose of the internet of things is primarily to use sensor data to make automated and optimised decisions. Accordingly, millions of datasets that must be protected in their entirety are generated. Staying with the example of the refrigerator, the collected data provides an interesting insight not only into the milk consumption of the household, but also into refrigerator use overall. Data like that could be used for marketing purposes. In extreme cases, the data would also indicate whether the eating behaviour of a household is healthy or unhealthy, which might be used by health insurers as an indicator for calculating premiums, for instance.

In the second half of 2016, the internet of things was in the news mainly because of a botnet called Mirai. A large number of poorly protected devices was hacked. On 21 October 2016, the infrastructure provider Dyn was attacked, resulting in outages of many popular internet services such as Amazon, Spotify and Netflix. This attack showed why the security of devices connected to the internet of things should not be neglected. The several hundreds of thousands of hacked devices were programmed to connect simultaneously with the services of the attack target. With a data traffic volume of 1.2 terabits per second, the attack was one of the strongest DDoS attacks ever observed.

In essential ways, the internet of things differs from conventional information and communication technology (ICT). Unlike computers, these internet-enabled everyday devices are often secured only inadequately against unauthorised access, which is why attackers are able to infect them with malware. Frequently, the default passwords of these devices can be exploited to infect them. These passwords are often not changed after installation, or they even cannot be changed at all. Another fundamental problem involves updates to the software employed: only rarely are there rules governing the update process, and even more rarely are updates automatic. This leads to numerous challenges that will become even worse over the coming years: unlike conventional ICT devices that are in operation for only a few years on average, internet things may often be used for up to 10 years or even longer.

3.3 Consequences for the future

The main risk to society is hardly that the internet of things will be misused for DDoS attacks, however. A much greater threat potential lies in the manipulation of such systems. Especially in the logistics sector, devices connected to the internet are booming. But the damage in that sector that might be triggered by manipulation is also enormous. If, for instance, manipulated pharmaceutical logistics deliver urgently needed drugs to the wrong location, this might very quickly become a matter of life and death. Criminals might try to extort money using attacks of this sort. And terrorists might try to intimidate and destabilise society with such attacks.

The problems relating to the security of the internet of things are primarily due to operators' lack of security awareness. At the last RSA security conference in San Francisco, security expert Lucas Lundgren once again pointed out the problem of poorly protected Message Queue Telemetry Transport (MQTT) communication.[4] MQTT is often used to ensure the communication of things using sensors. The problem is not the MQTT protocol as such. Rather, there are operators who simply do without password protection and encryption. In the case of battery-operated sensors, this failure might be explained with reference to higher CPU loads and thus higher power usage, but in many cases it is caused solely by ignorance or laziness.[5] Sensors with unsecured internet communications can be found in cars, earthquake sensors, ATMs, air conditioners, lighting and medical technology and other devices.

3.4 Guidelines and precautionary measures

The multitudinous uses of the internet of things in a wide range of industries, along with the immense and accelerating number of different devices, make it difficult to develop guidelines. Despite these challenges, the Cloud Security Alliance published a roughly 80-page report in October 2016.[6] The report provides an overview of the security functions available on the various software development platforms. The report also establishes guidelines for the design and production process, as well as a checklist that engineers can consult during the development process.[7] MELANI has also published several measures on its website intended to improve security in the internet of things.[8]

[4] https://www.rsaconference.com/events/us17/agenda/sessions/6671-lightweight-protocol-serious-equipment-critical (as at 28 February 2017)

[5] https://www.heise.de/newsticker/meldung/MQTT-Protokoll-IoT-Kommunikation-von-Reaktoren-und-Gefaengnissen-oeffentlich-einsehbar-3629650.html (as at 28 February 2017)

[6] https://cloudsecurityalliance.org/download/future-proofing-the-connected-world/ (as at 28 February 2017)

[7] http://www.inside-it.ch/articles/45282 (as at 28 February 2017)

[8] https://www.melani.admin.ch/melani/en/home/themen/internet_of_things.html (as at 28 February 2017)

Recommendation:

All devices connected to the internet must be secured (customised passwords, restricted access) and updated regularly. Updates should be installed as soon as they are available. Unlike in the case of a desktop computer or smartphone, however, hardly anyone remembers that intelligent light switches and refrigerators might also be devices requiring software updates.

An even greater threat potential comes from objects and devices that can be accessed from the internet using default access data (username and password). Such devices can in principle be found by anyone (e.g. using a port scan or a search engine like Shodan) and thus are an especially large target.

MELANI provides information on how to protect oneself from threats like these:

DOKU

Security in the internet of things (IoT)
https://www.melani.admin.ch/melani/en/home/themen/internet_of_things.html

4 Situation in Switzerland

4.1 Espionage

4.1.1 Switzerland as an indirect target of possible espionage activity

On 11 August 2016, Anonymous Poland announced that it had hacked the networks of the World Anti-Doping Agency (WADA) and the Court of Arbitration for Sport (CAS).[9] The group also claimed a DDoS attack against the CAS. The CAS, headquartered in Lausanne, is an international arbitration and resolution body for sports-related disputes. Doping is one of the current areas in which the CAS is frequently invoked. The facts of the case and the role played by Anonymous Poland are not yet completely clear. The interest in this arbitration body is obvious, however, given the exclusion of Russian athletes on doping grounds and the related political implications. Although Switzerland was not the actual target of this operation and the underlying circumstances affected it only indirectly, Switzerland is frequently the object of attention merely due to the fact that the CAS is located there. The high density of international organisations headquartered in Switzerland thus increases the risk of cyber operations. In the context of protecting its territory, Switzerland has to take this into account by appropriate means.

The publication of lists of infected domains and IP addresses on 13 August 2016 by a group calling itself "Shadow Brokers" is another case affecting Switzerland. The list included three addresses of servers at the University of Geneva. The servers were alleged to be connected

[9] See also section 5.1.2

to potential attacks by the "Equation Group".[10] The operator of Swiss university networks, Switch, confirmed that three servers were affected between 2001 and 2003. According to Switch, two of these servers had no longer been active since 2009, and the third had not been accessible externally.[11] Even though the case was already some time ago and measures have been taken in the meantime, it still shows that Switzerland is not only an attractive target, but also can be exploited as an intermediate stop and host of espionage infrastructure. Some of this infrastructure is housed at service providers who apparently do not take security that seriously[12], but it can also be placed by infecting legitimate servers.

In past semi-annual reports, we have repeatedly mentioned the factors that make Switzerland a popular target.[13] Concrete cases have also been pointed out in which the specific expertise or sensitive information of Swiss companies and institutions was targeted. The most prominent case that has recently come to attention is certainly the attack against the defence company RUAG[14]. But the cases described above also make clear that Switzerland can be a "collateral victim" of espionage activities in which Swiss interests are not targeted directly.

[10] See also section 5.1

[11] http://www.watson.ch/Digital/NSA/715933955-NSA-hackte-Uni-Genf-und-missbrauchte-drei-Server-f%C3%BCr-Cyberangriffe (as at 28 February 2017)

[12] This case is for example also reported in our semi-annual report 1/2014, section 3.3 https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2014-1.html (as at 28 February 2017)

[13] Especially see section 4.1 in the MELANI semi-annual report 2/2015, section 4.1 https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2015-2.html (as at 28 February 2017)

[14] MELANI semi-annual report 1/2016, section 4.1.1 https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2016-1.html (as at 28 February 2017)

Conclusion/recommendation:

In partnership with the private sector, MELANI has worked for 13 years on protecting against IT threats. For reporting incidents relating to information assurance, MELANI makes a reporting form available on its website:

REPORT

MELANI reporting form:

https://www.melani.admin.ch/melani/en/home/meldeformular/form.html

With its Prophylax programme, the Federal Information Service (FIS) is carrying out a prevention and awareness-raising campaign relating to non-proliferation and industrial espionage. It serves to raise the awareness of businesses and educational institutions:

DOCU

Prophylax programme:

http://www.vbs.admin.ch/de/themen/nachrichtenbeschaffung/wirtschaftsspionage.detail.publication.html/vbs-internet/de/publications/nachrichtendienst/Prophylax.pdf.html

http://www.vbs.admin.ch/de/themen/nachrichtenbeschaffung/wirtschaftsspionage.html

4.2 Data leaks

4.2.1 Extortion with supposed client data

In a press release on 17 November 2016, the Liechtenstein Bank Valartis disclosed that it had been targeted by a hacker attack. The attackers obtained various information on payment orders executed before May 2013 and primarily relating to business clients. The bank ruled out that payment orders had been manipulated at the expense of clients. The core system of the bank had not been affected by the hacker attack. The attackers had also not been able to access information about account balances and the like. Clients that might have been affected by the hacker attack had been informed by the bank. The bank learned of this attack when an individual contacted the financial institution by email and claimed to have discovered a data leak. That individual anonymously offered to close the security vulnerabilities against payment. Valartis did not accept the individual's offer or demands.[15]

Because the attacker was unsuccessful in obtaining money in this way, the attacker tried in a second step to contact the clients of the bank directly by email according to Inside-IT. The attacker did appear to have possession of at least some client email addresses. In an extortion letter, the attacker claimed to know account balances and other client data. In the event

[15] http://www.valartisbank.li/Download.aspx?mode=download&id=IqzI6qVOde5v%2foNBMJr8xg%3d%3d (as at 28 February 2017)

of non-payment, the attacker threatened to provide the data to tax authorities and the media. The extortionist demanded 10% of the account balance in the form of bitcoins.[16]

Because the clients had already been informed by the bank in advance, MELANI assumes that probably none of the victims met the extortionist's demands. An interesting detail is that the attacker would not have been able to verify whether the victims had actually transferred 10% of their account balance or less, because – according to the bank – the information had not been in the hands of the extortionist. The attacker was probably speculating on the victims' honesty in this regard.

Conclusion/recommendation:

In such cases, MELANI expressly advises against making a payment, as this might lead to dependency on the extortionist. At the same time, proactive communication is important to steal the attacker's thunder.

MELANI learned of similar cases several times in the period under review. In most cases, an SQL injection was used to access a poorly secured database in order to obtain the data. The motives of the attackers varied considerably: there are in fact some attackers who pursue this approach as a "business model", offering to close the security vulnerabilities against payment. In other cases, the whole story is merely an excuse to extort as much money as possible.

Hackers have tried to distinguish themselves by their backgrounds and motives. The terms "white hat", "grey hat", and "black hat" have become popular: white hats use their knowledge within the legal limits. Black hats typically act with criminal intent. They try to penetrate the target system – either to see whether they can, or possibly also to damage it or steal data. In between these two are the grey hats, who break the law, but with a higher motive, such as to force those responsible to take security more seriously and improve it. Grey hats often act illegally, but more or less according to "hacker ethics".

4.3 Industrial control systems (ICSs)

The central control of a house notifies the owner that the sunblinds have been closed at home. Upon learning of this, the homeowner immediately starts up the air conditioner remotely in order to return to a comfortable room temperature. Smartphones are often used to control these systems. As private users take more and more advantage of these conveniences, they increasingly enter into contact with building automation, a variant of industrial control systems.

What is increasingly being integrated into private households has long been standard in major complexes such as office buildings, factories and hospitals. Here, centralisation of the means for controlling an ever larger number of systems and devices is necessary to improve the quality and efficiency of administration. But this centralisation also increases the potential consequences in the event of unauthorised access and manipulation of the central control.

[16] http://www.inside-it.ch/articles/45798 (as at 28 February 2017)

4.3.1 Raising of awareness of threats facing networked ICSs

To take advantage of the convenience of remote maintenance, industrial control systems (ICSs) are often connected to the internet. This makes it easy to monitor the status of devices and issue control commands without having to be on site. If the connection to the internet is set up without adequate protection measures, there is a risk that the control systems will be operated by unauthorised third parties in an undesirable way. Specialised search engines such as Shodan[17] make it possible even for amateurs to discover such openly accessible systems. This cannot be in the interests of the operator.

If MELANI discovers such potentially threatened systems in Switzerland or if they are reported to MELANI, the operators are contacted to clarify whether they are aware of the accessibility of their system. In all cases, a recommendation to secure the control systems is issued.

At the end of last year, private security researchers reported an openly accessible building automation system to MELANI. The report claimed that it would be possible to gain unauthorised access to the building's climate control.

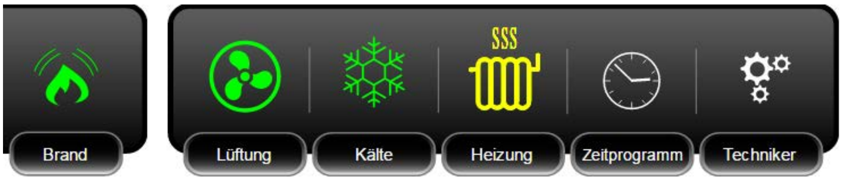


Figure 1: Detail of building control

Fortunately, it turned out that the control system in question was still in the testing phase. The building had not even been occupied yet. After concluding the last tests, the system was isolated from the internet and has since been accessible only to the technicians responsible for operation and maintenance.

Recommendation:

If you discover openly accessible control systems on the internet, notify us of the details so that we can contact the operator:

REPORT

MELANI reporting form:

https://www.melani.admin.ch/melani/en/home/meldeformular/form.html

DOCU

Checklist with measures for the protection of industrial control systems:

https://www.melani.admin.ch/melani/en/home/dokumentation/checklists-and-instructions/measures-for-the-protection-of-industrial-control-systems--icss-.html

[17] https://www.shodan.io/ (as at 28 February 2017)

4.4 Attacks

Individuals and companies in Switzerland continue to be targeted by different kinds of attacks. One important target is websites. Especially for companies that depend on a reliable presence on the internet, vulnerability to DDoS attacks and defacements can turn out to be problematic.

4.4.1 DDoS and extortion: current development in Switzerland

In the last MELANI semi-annual report, we drew attention to the different forms of extortion in connection with DDoS attacks. In the second half of 2016, the trend was confirmed that extortionists threatened their targets without even being able to carry out a DDoS attack. As expected, criminals immediately took advantage of the uncertainty incited by the major DDoS attacks carried out by the Mirai[18] botnet in order to extort bitcoins from victims. At the end of the year, a group supposedly called NewWorldHacker appeared and attempted to extort victims with an imminent attack. But no DDoS attack ever took place. As a reminder: the group NewWorldHacker had claimed responsibility for the massive attacks on the DNS provider Dyn.

Despite this trend, some other cases were a reminder that an actual attack can never be ruled out. Not necessarily all victims have to be attacked – it might be sufficient to make an example of a victim that serves as a warning to the other targets. A typical example of this approach is a group called DD-Crew DDoS, whose defining characteristic is that it focuses on a certain business sector. The attack is perpetrated solely against a single market participant in that sector. Referencing that attack, other businesses in the sector are then contacted individually and extorted into paying an amount in bitcoins so that they do not suffer the same fate as their competitor. Interestingly, the amounts of money demanded in these cases vary depending on the prominence (according to Google rank) and size of the company.

Conclusion:

The combination of extortion and threat of a DDoS attack will probably persist, and the fear of major attacks stoked by Mirai will probably continue to be exploited. Moreover, thanks to a variety of different services "offering" DDoS attacks (See section 6.1), any perpetrator can launch such attacks. This means that this criminal field of activity, with a multitude of perpetrators employing similar methods, is constantly in motion.

4.5 Social engineering, phishing

Apart from all the technical attacks, attacks that exploit human weaknesses are especially popular and successful.

[18] See section 3 and 5.4

4.5.1 Fraud attempts of differing quality

Several CEO fraud cases were again reported to MELANI in the second half of 2016. CEO fraud occurs if the perpetrator instructs the accounting or finance department in the name of the CEO or other manager to make a payment to an account that actually belongs to the scammers and typically is located abroad. [19] The reasons given for the payment differ, but the matter is usually claimed to be urgent and extremely sensitive and confidential. The quality of the cases of attempted fraud varies considerably. While in some incidents only a general request for an urgent transfer of funds is made, in other cases the scammers collect large volumes of information about the company to be attacked in order to make up a suitable story and carry out the fraud in a very targeted manner. An advisor or a bogus or supposed law firm is often also part of the scenario. To make the requests look serious, websites of banks or law firms are sometimes copied or imitated.

Federal offices were not immune from attack during the period under review. The finance divisions of the Federal Administration also received fraudulent instructions for fund transfers. In another case, the website of the Swiss Financial Market Supervisory Authority (FINMA) was imitated to induce the victims to make a payment.

That scammers are becoming increasingly tricky and are planning every detail of their attacks can be seen in cases where scammers even make phone calls claiming to be a federal office. The motivation is clear: by pretending to be an official government office, pressure can be exerted on the victim to perform an action desired by the attackers. Astonishingly, the number displayed on the victims' phone was actually that of the Federal Administration. The number was faked by the scammers.

Recommendation:

Social engineering attacks exploit the helpfulness, gullibility or insecurity of persons in order to gain access to confidential data, for instance, or to induce the victims to undertake certain actions. Of all the forms of attack, this is still one of the most successful. MELANI has published tips for protecting oneself from such attacks.

INFO

Current threats: social engineering

https://www.melani.admin.ch/melani/en/home/themen/socialengineering.html

4.5.2 Phishing

Numerous phishing emails were again sent out in the second half of 2016. The same types of email are repeatedly observed: some request credit card data for "verification" purposes,

[19] See section 4.5.2 of the MELANI semi-annual report 1/2016 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2016-1.html (as at 28 February 2017).

while others send the victim to linked pages requesting usernames and passwords for online services. Frequently, phishing emails also contain the logos of well-known companies or of the service in question so that the emails can be made to look official.

Overall, more than 4,500 different phishing sites were reported in 2016 using the antiphishing.ch portal operated by MELANI. Figure 2 presents the number of reported phishing websites per week, with variations of the number over the course of the year. The reasons vary: firstly, some of the fluctuations are due to holidays, as fewer phishing sites are reported during holidays; secondly, attackers regularly shift their attacks from country to country.

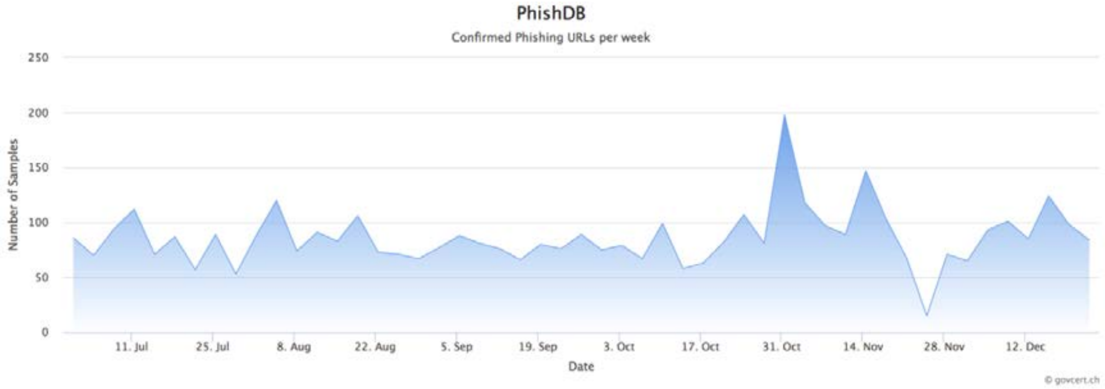


Figure 2: Reported and confirmed phishing sites per week on antiphishing.ch in the second half of 2016

4.5.3 Phishing sites that aren't

Already in semi-annual report 1/2012[20], MELANI pointed out how important it is to think through client communication in the age of phishing. It repeatedly happens that real emails to clients give rise to uncertainty. During the period under review, reports of supposed phishing sites by members of the public increased. This is in part certainly due to greater awareness of members of the public, but also because some companies do not abide by certain guidelines (see next info box).

4.5.3.1 The classic – changes to PayPal user agreement

Emails sent out by PayPal, eBay, etc. announcing changes to user agreements are a recurring occasion for reporting alleged phishing sites. Even if the email does not contain a link to a login page, the fact alone that users are receiving unexpected emails from PayPal gives rise to uncertainty and numerous reports to MELANI. This is probably not least because with regard to phishing PayPal is one of the internet services attacked the most often, and many users have in fact already received phishing emails purporting to be from those services.

4.5.3.2 Hidden link and link to third-party server

Emails from Swiss companies also triggered reports of supposed phishing sites to MELANI. During the period under review, a company sent out an advertising message saying that the

[20] MELANI semi-annual report 2012/I, section 3.8 https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2012-1.html (as at 28 February 2017)

client would receive a credit. But the link provided did not redirect to the company's website itself; it redirected to a domain of a company specialising in advertisement. Justifiably so, this caused recipients to be sceptical. In another case, a different company informed clients by email that a service fee would have to be paid if the recipient did not respond by a certain deadline. There was no personal salutation, and the hidden link redirected to a website where the user was asked to enter username and password. Many aware members of the public became suspicious and turned to MELANI. But the email was in fact from the company, and the link redirected to the company's website.

Conclusion/recommendation:

"No serious company will ever ask you for your username and password by email." This is the standard answer given by MELANI when people report an email and are unsure if it is actually from the company it claims to be from. This statement, which initially sounds simple, sometimes poses certain challenges to companies in the age of electronic client communication, however. How should a company communicate with clients so that they do not think it is a fraudulent email? And even more importantly: careless client communication by a company may also have a negative impact on client behaviour regarding fraudulent emails.

The following points should be noted by companies when sending out emails:

- Where possible, emails should be sent in plain text format so that any included links are clearly visible and are not hidden behind other text such as "click here".
- Use links sparingly in the email and only link to own domains. If possible, use links to encrypted pages (https) and communicate this to the recipient.
- Do not link to websites asking the user to enter username and password or other data.
- Send newsletter emails as regularly as possible.
- On the start page of the website, draw attention to the newsletter or link directly to the information so the recipient has the option of entering the main address manually and then clicking on the newsletter from there.
- Address clients by first and last name where available.

Especially in the financial sector, important information regarding accounts should be sent in writing by letter.

4.5.4 Increasing popularity of phishing awareness campaigns

Raising the awareness of one's own employees is key to ensuring the company's security. For that reason, more and more companies conduct phishing awareness campaigns. During such a campaign, manipulated phishing emails are sent to employees. The company then analyses who clicks on the links. This makes it possible for the company not only to make employees more aware, but also to determine the degree of awareness and take appropriate measures. The phishing site is saved on a domain acquired beforehand especially for that purpose. It makes sense that employees with a good level of awareness also forward such emails to anti-phishing reporting bodies such as the antiphishing.ch site operated by MELANI. But this process does trigger various measures such as web take-down processes and various entries in filtering programs. This reaction of course disrupts the awareness test. When websites are blocked or deleted, no information can be retrieved anymore about the degree of employee awareness.

Recommendation:

Thorough and repeated awareness raising of a company's employees, but also of the population, is one of the cornerstones of online security. Phishing awareness campaigns are one possibility for doing this. To guarantee a smooth campaign, at least all players involved with the infrastructure should be informed before the test is carried out: these include especially the registration authority for the top-level domain (SWITCH for .ch domains), the registrar and hosting provider, and any (external) email provider. Finally, it makes sense to announce the test to MELANI so that any reports can be responded to as desired by the organisers of the awareness campaign and so that no measures are taken by MELANI against the website.

4.6 Crimeware

Crimeware is a form of malware which, in criminological terms, ranks as computer crime and legally comes under causing damage to data and fraudulent misuse of a data processing system. Most infections in the second half of 2016 were due to Downadup (also known as Conficker). This worm has been around for over eight years and is spread via a security vulnerability in Windows operating systems that was both discovered and eliminated in 2008. Second most common are infections by the malware Necurs, which has specialised both in sending the encryption Trojan Locky and in the banking malware Dridex. In third place is the botnet Mirai, which infected devices in the internet of things and became known after its attack on the internet service provider Dyn.

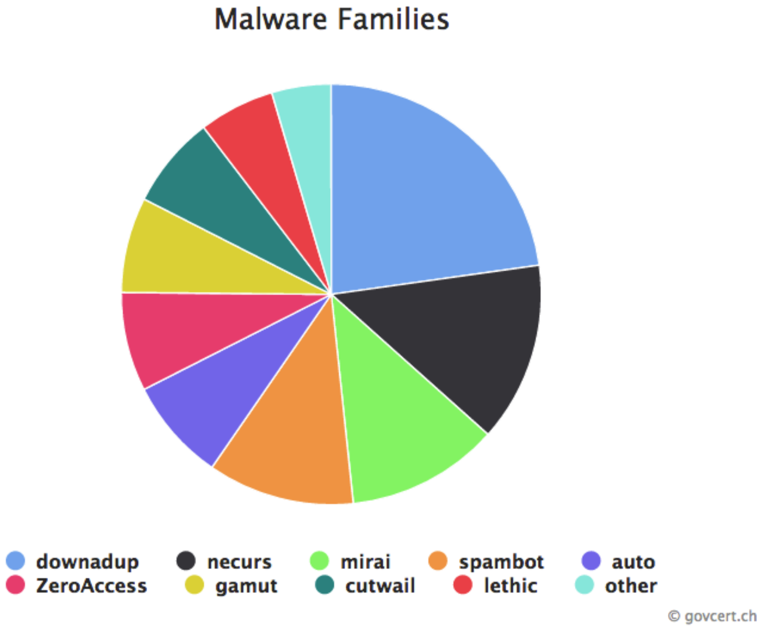


Figure 3: Distribution of malware in Switzerland known to MELANI. The cut-off date is 31 December 2016. Current data can be found at: http://www.govcert.admin.ch/statistics/dronemap/

4.6.1 Ebanking Trojans – focus on companies

The field of ebanking Trojan families did not change much in the last half year. The malware families Retefe and Gozi continue to be active in Switzerland. While Gozi is also spread via website infections, Retefe is spread using emails with fake bills of existing, more-or-less well-known companies. The attached Word document contains a JavaScript or executable file that changes the browser settings of Internet Explorer or Firefox, entering a proxy server belonging to the attackers. The attackers can then redirect any domain accessed by the user to a server of their choice as desired. Retefe also has the capacity to infect mobile phones in order to redirect a text message containing a mobileTAN to the scammers. According to reports of the security service provider TrendMicro,[21] the scammers have also refined the Android malware that intercepts the one-time password sent by text message. Criminals have now apparently endowed the malware with anti-analysis, device routing and remote access capabilities. The malware also tricks the user into giving the app certain rights, such as to the accessibility service, which permits the simulation of user interactions. Dridex is also sent by email with fake bills. Until June 2016, Dridex was used to attack only ebanking private clients, at least in Switzerland. The perpetrators changed their attack method in July 2016 and have since also targeted offline payment software solutions. Such software is used by many companies to transmit large volumes of payments via the internet to one or more banks. If the attackers discover such payment software after the initial infection, the specialised malware Carbanak is downloaded as well. A schematic overview of the infection path is presented in Figure 4.[22]

[21] http://blog.trendmicro.com/trendlabs-security-intelligence/new-smssecurity-variant-roots-phones-abuses-accessibility-features-teamviewer/ (as at 28 February 2017)

[22] The malware resurfaced at the end of February 2017 with a major spam wave: using fake Swisscom bills, the malware tried to trick recipients into installing the Trojan. https://www.govcert.admin.ch/blog/28/the-rise-of-dridex-and-the-role-of-esps (as at 28 February 2017)

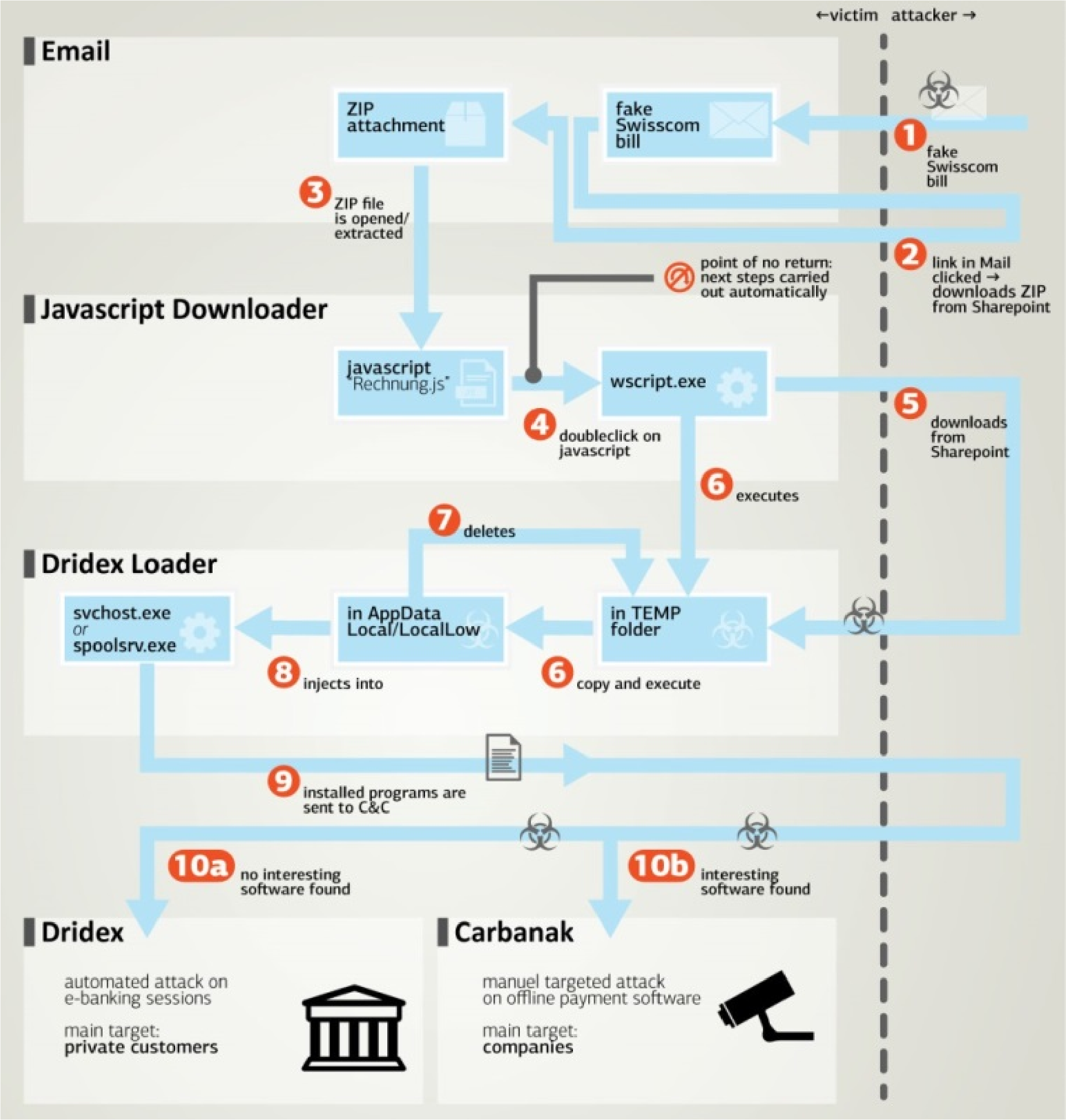

←victim attacker →
Email
ZIP attachment
fake Swisscom bill
1 fake Swisscom bill
2 link in Mail clicked → downloads ZIP from Sharepoint
3 ZIP file is opened/ extracted
point of no return: next steps carried out automatically
Javascript Downloader
javascript "Rechnung.js"
wscript.exe
4 doubleclick on javascript
5 downloads from Sharepoint
6 executes
7 deletes
Dridex Loader
svchost.exe or spoolsrv.exe
in AppData Local/LocalLow
in TEMP folder
8 injects into
6 copy and execute
9 installed programs are sent to C&C
10a no interesting software found
10b interesting software found
Dridex
automated attack on e-banking sessions
main target: private customers
Carbanak
manuel targeted attack on offline payment software
main target: companies

Figure 4: Schematic overview of the infection path during the spam wave with fake Swisscom bills in February 2017

Recommendation:

In the case of computers used for payment transactions, the following principles should be observed:

- For offline payment software and ebanking, use a dedicated computer that you don't use to browse the internet or receive emails.
- To authorise payments, use a joint signature via a second channel (e.g. ebanking). Ask your bank about available options.
- If you use a hardware token (e.g. smart card, USB dongle), remove it after using the payment software.
- Do not save ebanking and payment software access data (contract number, password, etc.) on your computer or in the software.
- Ask the manufacturer of your payment software about additional security measures, and activate automatic software updates.
- Immediately report suspicious payments to your bank.
- To prevent an infection with Dridex or other malware in your company, MELANI recommends the following measures:
    - Make sure that potentially harmful email attachments are already blocked or filtered on your email gateway or by your spam filter. Dangerous email attachments tend to use file extensions as listed in the following MELANI newsletter: https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/offline-payment-software.html
    - Make sure that dangerous email attachments such as these are also blocked if they are sent to recipients in your company in archive files such as ZIP, RAR or even in protected archive files (e.g. in a password-protected ZIP file).
    - Additionally, all email attachments that contain macros (e.g. Word, Excel or PowerPoint attachments with macros) should be blocked unless they are absolutely necessary. If feasible, the sending and receipt of such attachments could be limited to specific senders/recipients.

4.6.2 Ebanking Trojans take advantage of the carelessness of users

Even modern two-factor authentication such as CrontoSign, PhotoTAN and SecureSign are not immune to attempted fraud, even though these authentication methods are considered secure. At the end of November 2016, several cases were reported to MELANI in which hackers were able to exploit precisely these systems for fraudulent payments. Using social engineering, ebanking clients are tricked into authorising fraudulent payments via PhotoTAN, CrontoSign or SecureSign.

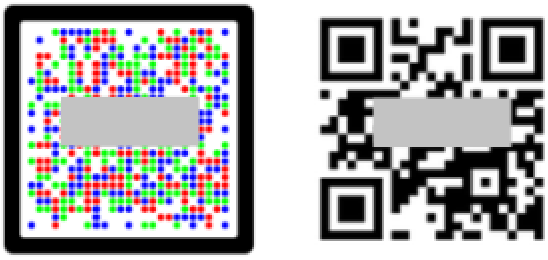
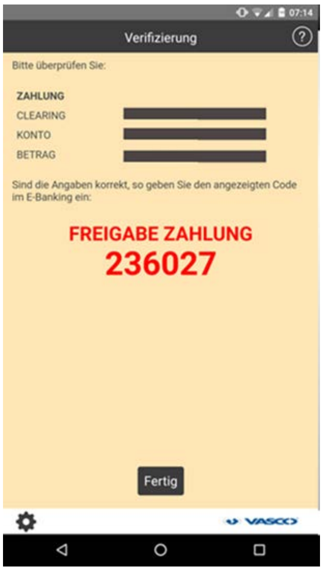


Figure 5: Mosaic (left) and QR code (right) used for login and authorisation of a payment

Clients are shown a QR code or mosaic in the ebanking portal when they log in or release a payment (see Figure 5). The client can scan the code with an app on a smartphone or dedicated device. Depending on the product, the login or authorisation of the payment is confirmed directly in the app, or the app generates a code that the client must enter in the ebanking portal. In many cases, however, clients are deceived by social engineering and end up authorising payments that could be recognised as fraudulent, for instance when an obviously false payee account is displayed in the app or if payment data is displayed already during the login process.

Manufacturers have responded by implementing improved visibility so that the user can distinguish even better between the login process and the release of a payment.



Bitte überprüfen Sie:

ZAHLUNG
CLEARING [redacted]
KONTO [redacted]
BETRAG [redacted]

Sind die Angaben korrekt, so geben Sie den angezeigten Code im E-Banking ein:

FREIGABE ZAHLUNG
236027

Figure 6: New, improved display of a one-time password generator, making clear that this is not a login, but rather the release of a payment.

Recommendation:

When using authentication methods involving smartphones, such as mTAN, PhotoTAN, CrontoSign and SecureSign, MELANI recommends the following:

- Ensure that, when you log in to ebanking, you are really confirming the login on your mobile device (e.g. smartphone or dedicated PhotoTAN devices), not already authorising a payment.
- If you are authorising a payment, always read the entire text on the mobile device and check the amount and payee (name, IBAN) on the payment before releasing it.
- Find out about other security measures offered by your financial service provider (e.g. default exclusion of payment to countries where you have no business relationship).

4.6.3 Ransomware

In the period under review, MELANI again received numerous reports of encryption Trojans. These included attacks against public administrations and SMEs. The key to dealing with ransomware attacks is a functioning backup on an external medium that cannot be affected by the encryption malware. But it is even better not to let things get that far and to take appropriate precautions. MELANI has published recommendations for that purpose (see info box below). Encryption and temporary loss of data are only part of the problem. It must also be taken into account that a large part of the company may not be able to work during the restoration of data from the backup. Because most companies today rely on functioning ICT, a standstill may result in substantial financial loss for the company. And in the case of critical infrastructures, a standstill of operations may have even much more serious consequences.

Especially the following ransomware types are widespread in Switzerland: Cerber, Locky and Mischa/Petya. One of the paths for distributing Cerber has been the supposed promise of winnings by email. An infection path that is also still very problematic is emails with supposed job applications sent specifically to human resource departments. Especially in HR departments, but also in media offices, employees have to open documents from unknown sources all the time. Here, it is recommended to operate computers isolated from the network and to print out the applications. But also attempts to use fake bills or fake court summonses are popular methods used by criminals. In general, scammers try to exploit qualities such as the victims' curiosity, fear and prospect of money or good luck.

Recommendation:

- Back up your data regularly. The backup should be stored offline, i.e. on an external medium such as an external hard disk. Make sure that the medium where the backup is saved is disconnected from the computer after the back-up procedure is complete.
- Always keep installed software and plug-ins up to date (e.g. antivirus programs, browsers).
- MELANI recommends that internet users not open suspicious email attachments, even if they come from supposedly trustworthy senders. In case of doubt, ask the (known) sender what the attachment is about.
- Offices whose function requires emails and attachments from unknown senders to be opened should use a dedicated computer that is isolated insofar as possible from the rest of the company's network for that purpose so that any infection cannot spread.

INFO

Measures against ransomware:

https://www.melani.admin.ch/melani/en/home/themen/Ransomware.html

Ransomware: Threat Situation, Prevention & Response from the German Federal Office of Information Security

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.html

No More Ransom project:

https://www.nomoreransom.org/decryption-tools.html

Rules of Conduct ➔ Email

https://www.melani.admin.ch/melani/en/home/schuetzen/verhaltensregeln.html

4.7 Preventive measures

4.7.1 Domains blocked on a preventive basis thanks to analysis of the malware Tofsee

Malware often contains a domain generation algorithm (DGA). The DGA's purpose is to generate domain names for the command and control servers (C&C), with which the infected computers (bots) then communicate. Dynamic and ongoing generation of domain names has the advantage versus fixed definition in advance that any measures taken against communication of the bots with the C&C infrastructure are much more complicated: first of all, the algorithm used has to be understood so that the domain names registered and used by the perpetrators can be predicted. At the end of December 2016, MELANI analysed the DGA of the malware Tofsee. It turned out that nearly half of the generated domain names used the top-level domain (ccTLD) .ch. The malware Tofsee is used for the broad dissemination of spam via infected computers. In cooperation with the registration authority Switch and the Registrar of Last Resort Foundation for combatting malicious domain names, MELANI was able to prevent the registration of more than 500 of the .ch domain names generated by the DGA over the course of 12 months.

4.8 Other topics

4.8.1 E-voting source code on GitHub

In December, the canton of Geneva published part of the source code for its e-voting system on the online service GitHub. The step was taken primarily for the purpose of transparency, but it may also lead to an improvement of the system thanks to external contributions. The Geneva e-voting system is also used in other cantons that have acquired it.

4.8.2 Switch remains registration authority for internet domain .ch

At the beginning of 2016, the Federal Office of Communications (OFCOM) published an invitation to tender for administration of the .ch domain names.[23] The SWITCH foundation was awarded the contract, as its offer achieved the highest number of points overall among the offers received.[24] It distinguished itself especially with its excellent concept for combating cybercrime. The registry function for the .ch domain names is already being performed by SWITCH. For at least another 5 years, it will now manage the national database of .ch domain names and ensure the electronic connection with the global domain name system (DNS).

The Federal Council has classified the Swiss top-level domain as a critical infrastructure. As such, it needs special protection because an outage would adversely impact large parts of public life in Switzerland. MELANI works closely together with the registry operator to guarantee the security and availability of Swiss domain names.

5 Situation internationally

5.1 Espionage

5.1.1 Attack on Democratic National Committee (DNC) in the US: official statement

Already in the last semi-annual report,[25] the cyberattack on the Democratic National Committee (DNC) in the United States was discussed. A report by the firm Crowdstrike had attributed these attacks to Cozy Bear and Fancy Bear.[26] In the second half of 2016, more information – apparently from the same campaign – was released on the platforms WikiLeaks

[23] https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-61133.html (as at 28 February 2017)

[24] https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-63597.html; https://www.switch.ch/news/SWITCH-wins-tender/ (as at 28 February 2017)

[25] Semi-annual report 2016/I, section 5.1.1 https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2016-1.html (as at 28 February 2017)

[26] https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/ (as at 28 February 2017)

and DCLeaks. In particular, this included about 58,000 emails from the infected account of Hillary Clinton's campaign manager, John Podesta.

In a joint statement on 7 October, the US Department of Homeland Security and the Office of the Director of National Intelligence accused the Russian government of using attacks on email accounts of political figures and institutions for the purpose of interfering with the US election.[27] An investigation report dated 29 December 2016 also referred to the Cozy Bear and Fancy Bear campaigns as the sources of the attack.[28] As a consequence, sanctions against Russian authorities and persons were announced.

What is special about this case is no doubt the specific way in which the Russian authorities were named by the highest level of another country as the authors of a cyberattack. Moreover, the resonance in the bitterly fought US presidential election was already heightened.[29]

5.1.2 APT 28 mentioned in connection with numerous incidents

The group referred to variously as Sofacy, Fancy Bear, Pawn Storm or APT 28[30] was suspected of being responsible for numerous other attacks in the period under review.

On 11 August 2016, Anonymous Poland announced that it had hacked the World Anti-Doping Agency (WADA) and the Court of Arbitration for Sport (CAS).[31] The precise identity and actual role of the group in this incident are unclear. On 19 August, the firm Threat Connect published an analysis which linked the attack to Fancy Bear.[32] This statement relied especially on the way in which the domain names were registered to imitate the two organisations.

In the case of WADA the attackers have used such domains for spear phishing attacks. The attackers tried to gain access to the Anti-Doping Administration & Management System containing information on doping tests of the athletes. The attack was confirmed by the agency. In particular, the attack succeeded in compromising the account of Yuliya Stepanova. With her revelations, the Russian runner had made the sanctions against Russian athletes possible in the doping case. In September, a group called Fancy Bear then published a large volume of data about athletes all over the world, supposedly from the WADA databases. WADA stated that some of that data might be falsified.

[27] https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national (as at 28 February 2017)

[28] https://www.us-cert.gov/security-publications/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity (as at 28 February 2017)

[29] See section 5.1 of the last semi-annual report 2016/I on interference with the last US presidential election: https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2016-1.html (as at 28 February 2017)

[30] These names were mentioned by the firms or authorities investigating the attacks

[31] The headquarters are in Lausanne. The case is discussed in the Switzerland section of this report.

[32] https://www.threatconnect.com/blog/fancy-bear-anti-doping-agency-phishing/ (as at 28 February 2017)

On 20 September, Süddeutsche Zeitung and the German radio stations NDR and WDR reported that German politicians had been attacked in August using spear phishing emails[33] purportedly sent by NATO. As was the case in the attacks against the German Bundestag in 2015, the newspaper cited sources close to the government attributing the attack to the espionage complex Sofacy. On 24 September, it was disclosed that Westdeutscher Rundfunk WDR had also been affected by the attack.[34]

In December, more reports appeared regarding incidents suspected of being authored by the same group. The newspaper Le Monde reported that the OECD had been targeted by an attack.[35] The OECD confirmed the attacks. At the end of December, Crowdstrike reported on Sofacy activities of a completely different magnitude.[36] The analysis of an Android app developed by a Ukrainian officer for the Ukrainian artillery[37] had shown traces of the malware x-Agent, which was used exclusively by Fancy Bear (alias Sofacy). With this infection for example, the positions of Ukrainian artillery installations could have been located more easily and potentially disarmed.

5.1.3 Winnti grows up – from stolen online gaming money to sophisticated industrial espionage against steelworks

At the beginning of December 2016, the German industrial conglomerate ThyssenKrupp disclosed to Wirtschaftswoche that it had become a victim of a cyber espionage attack.[38] Already in the spring, the group known as Winnti had succeeded in penetrating the company's networks. After discovery by the internal security team and six months of defensive work, the system had finally been cleaned up. But the attackers had succeeded in steeling several datasets.

The targets included locations of the Industrial Solutions corporate division in Europe, India, Argentina and the United States, but also the Hohenlimburg steel mill. Fortunately, there had not been any physical damage. The group's motives apparently were limited to spying.

The German Federal Office for Information Security (BSI) confirmed that there have been several cases involving Winnti that targeted other companies. The group is distinguished by its ability to infiltrate third-party system environments through well-hidden remote access. Winnti gained notoriety in 2009 with attacks on online games where gaming money was di-

[33] http://www.sueddeutsche.de/politik/bundesregierung-ist-alarmiert-hackerangriff-aufdeutsche-parteien-1.3170347 (as at 28 February 2017)

[34] http://www.spiegel.de/politik/deutschland/cyberattacke-russische-hacker-attackieren-wdr-journalisten-a-1113780.html (as at 28 February 2017)

[35] http://www.lemonde.fr/international/article/2016/12/28/l-osce-victime-d-une-attaque-informatique_5054744_3210.html (as at 28 February 2017)

[36] https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/ (as at 28 February 2017)

[37] The app had been distributed on military forums and was claimed to improve the deployment of D-30 howitzers

[38] http://www.wiwo.de/unternehmen/industrie/spionageangriff-auf-thyssenkrupp-grossalarm-haette-die-risiken-erhoeht/14948264.html (as at 28 February 2017)

verted and subsequently sold on the black market. Since 2015, it has apparently expanded its activities to include cyber espionage against companies.

5.1.4 NetBotz – the camera that monitors more than just the view frame

Monitoring technology manufactured by the US firm NetBotz – such as surveillance cameras and server monitoring systems – is frequently used in especially sensitive areas of public authorities and major companies. According to the German ARD magazine Fakt, however, these devices include secret access points for US intelligence services.[39] Fakt cites a report of the German Federal Intelligence Service (BND) classified as secret. The report states that already in 2004 the BND had received information from a source about the possible backdoor in NetBotz products. A technical analysis apparently verified that the NetBotz system was trying to establish a covert connection with a server of the US Department of Defense. NetBotz apparently used aggressive low-price offers to try to sell its products to the German Federal Foreign Office and potential clients in the high-tech and defence industries. The investigative magazine criticises especially that the BND didn't inform the Bundesamt für Verfassungschutz (BfV, the domestic intelligence service of Germany) or the affected companies of its findings regarding the covert remote access. NetBotz is now part of the French company Schneider Electric, which manufactures many elementary components of a wide range of industrial control systems.

5.1.5 Other campaigns in the headlines

Sofacy was certainly one of the espionage campaigns mentioned the most in the last six months of 2016. But numerous other cases of cyber espionage were uncovered all around the world. They were usually published by security firms based on research conducted for the affected clients. Because we cannot mention all of the many campaigns here, we will focus on a few examples: according to Kaspersky, the not very sophisticated espionage complex Dropping Elephant[40] comes from India; On the StrongPity[41] primarily targets encryption systems; and Symantec has reported on the activities of a group called Strider[42] (also referred to by Kaspersky as ProjectSauron[43]), which carries out sophisticated attacks against a few selected targets. Finally, an Israeli group (NSO Group) was accused of exploiting vulnerabilities in the iPhone for surveillance purposes. Apple subsequently fixed the vulnerabilities.[44]

Also worth mentioning are tools and malware allegedly from the arsenal of the Equation Group, published by a group named Shadow Brokers on 13 August 2016. As a reminder: Equation Group is a group engaged in sophisticated cyber espionage suspected of being backed by the NSA. Shadow Brokers claimed that the published material was only part of

[39] http://www.mdr.de/fakt/industriespionage-100.html (as at 28 February 2017)

[40] https://securelist.com/blog/research/75328/the-dropping-elephant-actor (as at 28 February 2017)

[41] https://securelist.com/blog/research/76147/on-the-strongpity-waterhole-attacks-targeting-italian-and-belgian-encryption-users (as at 28 February 2017)

[42] http://www.symantec.com/connect/blogs/strider-cyberespionage-group-turns-eye-sauron-targets (as at 28 February 2017)

[43] https://securelist.com/analysis/publications/75533/faq-the-projectsauron-apt/ (as at 28 February 2017)

[44] https://motherboard.vice.com/en_us/article/nso-group-new-big-player-in-government-spyware?trk_source=recommended (as at 28 February 2017)

what was in their possession, and that the rest would be auctioned off. Numerous experts subsequently confirmed the authenticity of the files. On 31 October, the group published a new archive with infected domain names and IP addresses that were allegedly used to carry out attacks.[45] There is considerable speculation about the identity of Shadow Brokers and the origin of the information.

Attribution of sophisticated attacks (of the type APT) is usually undertaken based on technical elements (typically the infrastructure used) or very specific approaches employed. The reliability of these attributions varies considerably. The initial appraisal must often be supplemented by considerations of a political and strategic nature. The targets of attacks are not necessarily chosen randomly, but rather in accordance with a specific pattern. The reason why a perpetrator might be interested in a specific organisation must be ascertained. If the answer to that question applies not only to an isolated case, but rather to an entire constellation of cases, then attribution of the attacks becomes easier.

5.2 Data leaks

Data is one of the raw materials – if not the raw material – of a digital economy and society. Virtually every company operates a database with a large volume of personal (client) data. Adequate account must be taken of security. Despite this, data leaks, i.e. unauthorised data gathering, are regularly brought to the attention of the public.

5.2.1 Yahoo data breach – an unimaginably large data leak

In mid-December 2016, Yahoo announced a data leak of nearly unimaginable magnitude. In an incident dating back to 2013, unknown perpetrators had accessed more than a billion datasets. Fortunately, the data did not include credit card information. But data such as names, dates of birth, telephone numbers and email addresses still has value in criminal circles. The data forms the basis for further social engineering attacks. This also explains why attackers are increasingly frequently connecting names with email addresses in order to address recipients personally. Already in September 2016 Yahoo announced a data breach dating back to 2014, which has affected 500 million Yahoo user accounts.

5.2.2 Data leak by insiders

The Sage Group is known worldwide as one of the largest suppliers of business and finance software for small and medium-sized enterprises. The attack on The Sage Group, which apparently took place at the beginning of August 2016, affected datasets of up to 300 companies using Sage's finance software. Sage stores a wide range of its clients' data, including names, addresses, dates of birth, social insurance numbers, account information and other financial data. Because access was gained using a regular login, it was assumed from the outset that the crime was perpetrated by an insider. This assumption was in fact confirmed.

[45] See chapter 4 on the extent to which Switzerland was affected

The incident once again makes clear to every security officer that – in addition to protection against attacks by outsiders – attacks by insiders should not be neglected.

5.2.3 AdultFriendFinder attacked again

The adult portal AdultFriendFinder again became a victim of unauthorised data access. In November 2016, a leak of a total of 412 million datasets was announced. Already in 2015, the portal made the headlines because of a similar incident involving 3.5 million datasets. Especially data from adult sites is a lucrative business for criminals and can be used for profit. According to the portal LeakedSource, the stolen data includes email addresses, passwords (some of which are unprotected), usernames, IP addresses and browser information.[46] LeakedSource condemned the fact that the provider had not encrypted the data properly and had stored the passwords in plain text or using the obsolete hash function SHA 1.

[46] http://www.leakedsource.com/blog/friendfinder (as at 28 February 2017)

Recommendation:

Looking at the email addresses surfacing in such hacked databases, it becomes apparent that many of them are corporate email addresses, even though the internet service in question most likely has nothing to do with the account holders' work. Many companies permit reasonable private use of company infrastructure – especially internet access. The use of company email addresses for private purposes should be subject to clear rules, however. The use of company IT for the purpose of private email communications may also be dangerous: suspicious attachments should not be opened either in the office or at home.

INFO

Rules of conduct for email

https://www.melani.admin.ch/melani/en/home/schuetzen/verhaltensregeln.html ➔ Email

INFO

Rules of conduct for passwords

A password should be changed regularly (about every three months), but at the latest if you suspect that it might be known to a third party.

Other rules: https://www.melani.admin.ch/melani/en/home/schuetzen/verhaltensregeln.html➔ Password

If you as a company administer client databases yourself that clients can access online, you should ensure that you do not become the victim of the next data leak. Use the checklist on our website for help.

DOCU

Checklist on IT security for SMEs

https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/checkliste-online-auftritt-kmu.html

INFO

SME portal of the federal government

https://www.kmu.admin.ch/kmu/en/home.html

5.3 Industrial control systems (ICSs)

The key topic of this semi-annual report takes a closer look at the internet of things. But things linked together with network technology have already been in use for a long time. Sensors and actuators are centrally coordinated, automated and optimised using control systems. Those systems control power grids, traffic flows, building air conditioning and medical technology in hospitals.

5.3.1 Déjà vu in Kiev – another power outage in Ukraine

Almost exactly one year after the power outage in parts of Ukraine at the end of 2015, which we discussed in the semi-annual report before last,[47] the lights went out again in the north of Kiev. Once again, shortly before Christmas – on Saturday, 17 December 2016 – and shortly before midnight, customers of the state power company Ukrenergo supplied by the Pivnichna substation were without electricity for nearly an hour.[48] Ukrenergo informed its customers that it was unclear whether component failure or a hacker attack was the cause of the outage. A few weeks later, Oleksandr Tkachuk, Ukraine's security service chief, said that both the power outage as well as attacks on the financial system and other infrastructures had been orchestrated by Russian security services in collaboration with private software companies and cybercriminals.[49] According to Tkachuk, the attacks had been constructed by the same persons who had been involved in earlier attacks using the BlackEnergy malware. His claims have not yet been verifiable by independent specialists. The accusations have so far been supported only by Ukrainian security researchers at Information Systems Security Partners (ISSB) as well as Honeywell Cyber Security Labs at a speech held during the ICS security conference S4 2017.[50] According to their own statements, these specialists were involved in the investigation of the incident. They claimed that the remote terminal units (RTUs) had not been rendered inoperable by overwriting of their firmware as they had the year before. In the more recent attack, they were simply shut down remotely, which is why it had been possible to restore power more quickly. According to the security researchers, the attackers had had the capacity to cause significantly graver damage. To that extent, the attack had not aimed to achieve maximum damage, suggesting that it was more of a demonstration of force by the saboteurs.

The targets had been infiltrated by malware using a massive email campaign in July 2016. Afterwards, the attackers spent several months in the networks, analysing them and making their way towards the target devices. Apart from the power supplier, the Ministry of Finance and the State Treasury had been victims, as well as Ukraine's state pension fund. On 6 December 2016, a DDoS attack was carried out against these targets, while internal network components were damaged and databases were destroyed. This resulted in an interruption and delay of state payment transactions.

[47] MELANI Semi-annual report 2015/II https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2015-2.html (as at 28 February 2017)

[48] https://motherboard.vice.com/en_us/article/ukrainian-power-station-hacking-december-2016-report (as at 28 February 2017)

[49] http://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN15U2CN (as at 28 February 2017)

[50] https://www.youtube.com/watch?v=lTwsDLO3C44 (as at 28 February 2017)

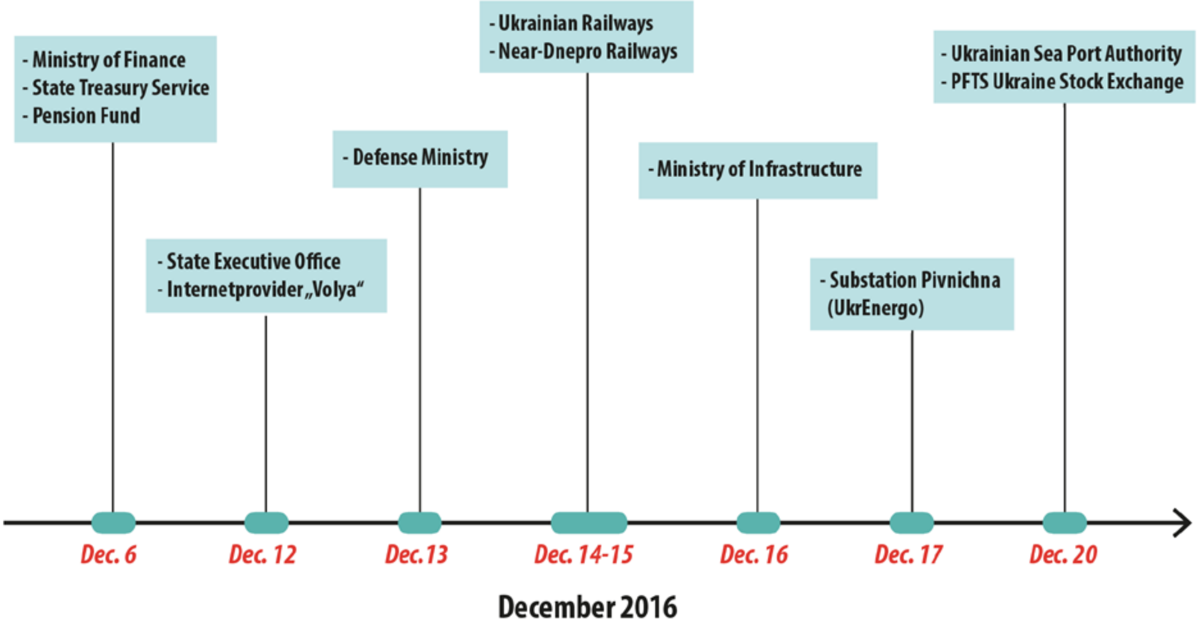


Figure 7: Time axis of the various attacks (source: S4 Events)

On 14 December 2016, the Ukrainian state railway network operator was also targeted by saboteurs. Once again, a DDoS attack was launched as a distraction, targeting the online ticket shop. In the meantime, the automated cargo management of freight trains was manipulated. Researchers see parallels with the 2015 attack because of the observed strategies used by the saboteurs to spread through the infiltrated networks. They noted progress in regard to the macro viruses contained in the targeted email attacks. Compared with the simpler macros in 2015, only 1% of the code was used for actual functionality. 30% of the program code was intended to make analysis more difficult, and a further 69% served solely to conceal the malicious nature of the malware.

The security researchers involved gained the impression that Ukraine was being used as a training ground for such cyberattacks, in which the opposing side tested its capacities. The security researchers say that an in-depth analysis of the incident will take a few more months. Until then, the findings presented will hardly be available for verification by independent specialists.

In the context of industrial control systems, caution should be exercised primarily in regard to the alarmism that tends to arise when apparently spectacular attacks are discovered. This is the view of Robert M. Lee, who participated in the analysis of the 2015 incident. If appropriate security measures are implemented consistently, even attacks that are frightening in terms of their effects can be discovered and prevented. For instance, the cyber security firm SentinelOne had to issue a correction of one of its malware analyses after the press had used it as a basis for claiming that state attacks had been perpetrated against the US energy sector. The only indication of that had been the fact that one of the victimised systems also had been running an energy management system. The malware itself did not have any features that specifically targeted the control systems, however.

5.3.2 Distributed denial of heating – freezing after a DDoS attack

In the city of Lappeenranta in the east of Finland, the residents of two buildings had to do without heat and warm water for an extended period of time. The reason for the outage was a DDoS attack that affected the superordinate building automation control system in a disastrous way.[51] The system tried to stop the attacks by rebooting, but it ended up in an infinite loop, and the heat stayed shut off. In their search for unsecured configurations or vulnerabilities of devices, botnet operators had stumbled upon Finnish building automation control systems. The heat was finally reactivated once data transmission was slowed down at the superordinate network levels and the DDoS attack could be defeated in that way. The manufacturer of the system stated that several attacks of that kind had been observed in the country.

Secure operations would be possible if the system were operated in isolation as recommended. For reasons of convenience and easier use, however, these systems are frequently connected with the internet.

Conclusion/recommendation:

The increasing computerisation and networking of all sorts of objects of everyday use (internet of things) offers many new and useful functions and conveniences. However, the associated risks should not be ignored. New possibilities always entail dangers as well, which must be taken into account already during the development phase (security by design).

DOCU

Checklist with measures for the protection of industrial control systems

https://www.melani.admin.ch/melani/en/home/dokumentation/checklists-and-instructions/measures-for-the-protection-of-industrial-control-systems--icss-.html

5.4 Attacks

5.4.1 Internet outage affects 900,000 Deutsche Telekom customers

On 27 November 2016, a worldwide attack against numerous home network routers was reported. The attack resulted in an internet outage for 900,000 Deutsche Telekom customers in Germany. The reason for the outage was the deployment of a new version of the malware Mirai, which had already been used for the attack against the DNS servers of the company Dyn on 21 October 2016.[52] Mirai is a malware targeting the Linux operating system, which is mainly used in devices in the internet of things. In this case, the malware searched the home network routers of end customers, looking for a vulnerability to install the malware. Because home network routers of Deutsche Telekom have a proprietary operating system, it turned

[51] http://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter (Stand: 28 February 2017)

[52] See key topic chapter 3

out to be impossible to install the malware. But the numerous attack attempts did manage to crash the devices. Deutsche Telekom provided a software update to its clients.

5.4.2 Targeting financial transactions

During the period under review, several cases in which criminals tried to manipulate financial transactions made the headlines. The following examples show how diverse the potential targets of such attacks are.

On 6 November, the UK Tesco Bank disclosed that malicious activities had been detected involving about 40,000 accounts, about half of which suffered losses. The bank was forced to take emergency measures and stop the transactions. Even a few months later, there are still open questions regarding the precise approach taken by the attackers. There was criticism in the UK about the bank's lack of communication. In addition to compensation for affected clients, the bank might have to deal with other financial consequences, since the UK financial market regulator may fine the bank depending on who is at fault in this case.

In addition to attacks directly targeting banking systems and especially the payment system SWIFT,[53] ATMs have also become possible targets of cybercriminals. In Thailand, a total of 12 million baht (the equivalent of CHF 343,000) was stolen in a series of attacks in August 2016. In an analysis, the security service provider FireEye concluded that a malware called Ripper[54] was most probably responsible for the attack. Once Ripper is installed in the system of an ATM, the malware must be activated with a manipulated chip card. This is evidence of a striking degree of organisation on the part of the criminals, who first have to compromise the ATMs, manufacture the cards and finally gain physical access to the ATMs. In November, the security firm Group-IB published a report about a group of perpetrators named Cobalt that is suspected to be behind a series of incidents in Europe. In those cases, money was withdrawn from the ATMs after the systems of several banks had been compromised.[55] The special aspect of these attacks is that they are thought to have been perpetrated without physical manipulation of the ATMs.

As already mentioned in earlier reports, greater success has also made services relating to digital currencies a target of attacks.[56] During the period under review, the cryptocurrency exchange Bitfinex was targeted by a massive attack resulting in the theft of 120,000 bitcoins, which at the current exchange rate (February 2017) is equivalent to more than CHF 130 million. For the attack to be successful, the perpetrators had to infect the multiple-signature system used by Bitfinex clients. The impact of the theft on the markets was swift: bitcoin prices fell by 13% within two days after the report was published.

[53] See semi-annual report 2016/I, section 5.4.1 "Cyber bank robbers steal USD 81 million", https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2016-1.html (as at 28 February 2017)

[54] https://www.fireeye.com/blog/threat-research/2016/08/ripper_atm_malwarea.html (as at 28 February 2017)

[55] http://www.reuters.com/article/us-cyber-banks-atms-idUSKBN13G24Q (as at 28 February 2017)

[56] See semi-annual report 2014/I, section 4.10, "Attacks targeting virtual currencies", https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2014-1.html (as at 28 February 2017)

Finally, the trend of further development of the group associated with the Carbanak malware was confirmed. Carbanak was in the headlines in 2015 after massive attacks on banks.[57] According to Trustwave researchers,[58] the malware targeted the hotel sector in 2016. With the help of spear phishing attacks, sales terminals were apparently infected in order to subsequently gain access to credit card data.

Conclusion:

The developments observed over the past years show that the end customer is no longer the only potential vulnerability in the payment chain. Banks themselves are often directly targeted by attackers via their internal systems or ATMs. Cybercriminals are also targeting the new, exclusively digital currencies.

5.4.3 Ransomware market continues to be very fragmented

The second half of 2016 was very dynamic for ransomware, as chapter 4 of this report shows. Numerous reported incidents at the international level testify to a wide range of attacks, targets and approaches. The entrepreneurial logic pursued by these criminals was described in our last report. They are steadily improving their products and looking for new opportunities, and even resort to providing "customer service" for their victims. This is done using FAQs, for instance,[59] or by establishing a direct dialogue with the victims. The ransomware market with multitudinous groups and very differing goals and approaches is apparently still in a consolidation phase. This is different in other cybercrime areas such as banking Trojans, where several well-established groups meanwhile appear to be divvying up market share.

One case that stood out in the last half year concerned the San Francisco transport system. On 25 November 2016, an attack disabled the ticketing system. The operators were forced to transport passengers for free until the systems were restored from a backup. The attacker had also claimed to be in possession of sensitive data, but that was denied by the operators. Several days later, additional information[60] was used to establish a clearer profile of the perpetrators, who evidently were also responsible for other attacks of this kind. The attackers were apparently not specifically targeting the San Francisco transport authority, but rather were simply looking for vulnerable systems.

[57] See semi-annual report 2015/I, section 5.1.2, "Carbanak – the electronic bank robbery", https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2015-1.html (as at 28 February 2017)

[58] https://www.trustwave.com/Resources/SpiderLabs-Blog/New-Carbanak-/-Anunak-Attack-Methodology/ (as at 28 February 2017)

[59] List of answers to questions that victims might ask are included in the extortion message

[60] https://krebsonsecurity.com/2016/11/san-francisco-rail-system-hacker-hacked/ (as at 28 February 2017)

Conclusion:

Even attacks against office automation systems that were not originally targeted may trigger chain reactions and cause concrete damage. The problem in such cases is not so much the restoration of the systems as such, but rather the time required to do so. During that time, temporary solutions and effective crisis management must be implemented.

5.5 Vulnerabilities

In addition to numerous vulnerabilities published in the second half of 2016, this report examines three that are illustrative of the vulnerability of our systems and programs in three different areas.

5.5.1 Vulnerability in the USB port

Everyone knows that plugging someone else's USB stick into your own computer poses a risk and is generally a bad idea. Operating systems are meanwhile set up so that they no longer automatically execute files on a USB stick but rather ask the user first what should be done. But what if precisely this security element is disabled? As security expert Samy Kamkar explains in his blog,[61] attaching a USB device he manipulated can serve as the gateway to install malware. This works even if the computer is locked. The software developed by Kamkar purports to be an Ethernet device attached to the USB port, simulating an Internet-over-USB connection. This makes it possible not only to tap cookies and hijack internet communications, but also to install a permanent backdoor. The only precondition for a successful attack is that a browser has been installed on the computer.

Conclusion/recommendation:

How often have you left your computer unattended at a conference, in a library or in a café during a lunch or toilet break? Especially for targeted espionage attempts, this would be an optimal opportunity for an attacker. Countermeasures are to never leave the computer unattended or to deactivate the USB and other ports.

5.5.2 Password managers – a key vulnerability?

There has been a lot of debate regarding the use and security of password managers. Some swear by this tool, because it makes it possible to use very secure, long and complicated passwords. Some programs even notify the user when passwords are due to be changed, or they recommend a secure password. Only the master password has to be remembered. This is exactly where sceptics raise their concerns: if attackers are able to steal the database or crack the master password, they have immediate access to all passwords – a goldmine for criminals. It would be even worse if the password manager contained a vulnerability. Such a vulnerability was in fact found at the end of July 2016 in the Firefox add-on of the LastPass

[61] https://samy.pl/poisontap/ (as at 28 February 2017)

program.[62] Visiting a manipulated website made it possible for the attackers to access the user's passwords. The vulnerability was closed.

5.5.3 Masque attacks in iOS

"Masque" attacks were seen for the first time in 2014, allowing hackers to replace a real app from the Apple App Store with a manipulated, company-signed app with the same bundle identifier.[63] This allows criminals to create malicious content with the same bundle ID as the original. If the original is popular, this of course also increases the range and the probability that the user will download this manipulated app. The vulnerabilities responsible were closed by Apple, but TrendMicro noted numerous new manipulated apps.**[64]** A report published in November 2016 examines the reasons: criminals are exploiting a function in the signing process that allows them to achieve data inheritance. The problem was eliminated in iOS in co-operation with Apple, but devices running iOS 9.3.5 or earlier are still vulnerable.

5.6 Preventive measures

Apart from raising awareness among users, capturing cybercriminals is the most effective measure for preventing cybercrime. Many people believe that identifying and capturing perpetrators is difficult or even impossible. But success has been achieved in this regard as well.

5.6.1 Avalanche network: arrests and house searches

Since 2009, criminals had used the international criminal network named Avalanche to carry out malware, phishing and spam activities. Each week, they sent more than 1 million emails with malicious attachments or links to unsuspecting victims. The Avalanche network was also used as a delivery platform for coordinating global mass attacks and recruiting financial agents. The total worldwide damage is estimated to be several hundred million euros, but the actual damage is difficult to assess, given that different malware families were administered using this portal. Investigations of the platform began in 2012. On 30 November 2016, the infrastructure was disabled. Investigators from 30 countries were involved in the deactivation of the platform. 5 people were arrested, 37 houses were searched and 39 servers were confiscated. Prosecutors were able to identify victims in more than 180 countries. 221 servers were shut down after the providers were contacted and requested to take them down.[65]

[62] https://blog.lastpass.com/2016/07/lastpass-security-updates.html/ (as at 28 February 2017)

[63] A bundle identifier is an expression for identification which is defined when developing an app and subsequently maintained, usually in the form of com.your-company.app-name

[64] http://blog.trendmicro.de/masque-attack-missbraucht-das-code-signing-in-ios-fuer-faelschungen/ (as at 28 February 2017)

[65] http://www.staatsanwaltschaften.niedersachsen.de/download/113197 (as at 28 February 2017)

Conclusion:

The example shows that law enforcement authorities can act successfully against cybercrime in particular if they work together internationally and also with private firms.

5.7 Other topics

5.7.1 End of US supervision of global internet address administration

On 30 September 2016, the historic supervision role of the United States over the administration authority for internet addresses (ICANN) came to an end.[66] Worldwide internet address administration has since been supervised by a globally composed community in which all stakeholders are represented. With this important step, international multi-stakeholder administration of the domain name and internet protocol address system (DNS) has come closer to reality.

Under the IANA contract[67] between the US government and ICANN, the US government had exercised overall supervision of DNS administration since 1998. In that way, it played a verification and validation role regarding changes to the central database of all top-level domains (such as .swiss, .com, or country codes such as .ch). The IANA contract expired at the end of September 2016 and was not renewed.[68]

The new institutional framework, which is intended to ensure global and more democratic supervision of the internet, grants the ICANN sub-organisations (including the Governmental Advisory Committee GAC, in which Switzerland is represented by OFCOM) certain oversight powers over the ICANN Board: blocking the budget, approval of amendments to the statutes, and recalling of the Board and individual members.

ICANN continues to be headquartered in California and is thus primarily subject to US law and intervention by US authorities. Nevertheless, this step is an important milestone in the transition of ICANN towards becoming a global institution. Other steps to strengthen its diversity and to take account of the needs and interests of the global community are necessary, however, and are suggested and supported by OFCOM as well as other Swiss stakeholders.

Internet users are not likely to notice much about these changes, however, because this transition does not affect the everyday technical functioning of the DNS.

[66] https://www.bakom.admin.ch/bakom/de/home/das-bakom/medieninformationen/bakom-infomailing/bakom-infomailing-43/us-aufsicht-ueber-die-globale-netzverwaltung-beendet.html; https://digitalwatch.giplatform.org/processes/iana (as at 28 February 2017)

[67] https://www.ntia.doc.gov/files/ntia/publications/ianacontract.pdf; https://www.icann.org/en/system/files/files/contract-01oct12-en.pdf (as at 28 February 2017)

[68] https://www.icann.org/news/announcement-2016-10-01-en (as at 28 February 2017)

5.7.2 Internet exchange point operator DE-CIX wants judicial review of surveillance measures

The operator of the Frankfurt internet exchange point DE-CIX has sued the Federal Republic of Germany at the Federal Administrative Court in Leipzig.[69] The lawsuit requests judicial review of the practice of strategic telecommunication surveillance by the Federal Intelligence Service (BND).

The lawsuit is based in part on an expert opinion[70] by Dr Hans-Jürgen Papier, a professor of law and former president of the Federal Constitutional Court. He expresses serious doubts concerning the legality of current practice and asserts that telecommunication secrecy should be considered a human right. To that extent, this right should also be accorded to foreigners, and any limitation must be formally provided by law. Opposing this view, the German government asserts that no law is required for the surveillance of purely foreign data.

In Switzerland, the Intelligence Service Act was established as the formal basis for the wire surveillance of foreign telecommunications. Any measure in this regard must be approved not only by the Head of the DDPS, but also by the Federal Administrative Court, and is thus subject to both political and independent judicial oversight.

6 Trends and outlook

6.1 Cybercrime-as-a-service and cyber extortion: a vicious circle

Cybercrime-as-a-service consists of a range of services for carrying out a cyberattack without special expertise. These services include the use of a wide range of malware, rental of a botnet, execution of a DDoS attack, money laundering services, etc. The phenomenon is not new – numerous such services have been available in underground forums for several years. But until recently, they had been limited mainly to closed cybercriminal groups, which used them to ensure more efficiency by dividing labour. This type of organisation allows perpetrators to specialise and to refine their special skills in order to offer them for sale or exchange.

With the emergence of cyber extortion, the situation has developed further. A whole new range of services on the market has opened up the options. As an example, let's look at extortionate DDoS attacks: today, practically anyone can buy a stresser/booter service[71] to carry out such an attack. Extortionists merely have to select the target and a form of attack, with different levels of effectiveness and prices. Even the use of a botnet with objects compromised by Mirai can be bought. This is similarly true of ransomware. This type of attack is

[69] https://www.de-cix.net/de/about-de-cix/media-center/press-releases/information-on-the-lawsuit-against-the-federal-republic-of-germany (as at 28 February 2017)

[70] http://rsw.beck.de/rsw/upload/NVwZ/NVwZ-Extra_2016_15.pdf; https://netzpolitik.org/2016/ex-praesident-des-bundesverfassungsgerichts-bnd-zugriff-auf-internet-knoten-wie-de-cix-ist-insgesamt-rechtswidrig/ (as at 28 February 2017)

[71] "DDoS-as-a-service" can be rented and is sometimes offered online labelled as "stress tests"

available "ready to use" and can also be carried out by individuals without technical expertise.

In light of this situation, the question arises as to the dynamics of the market: has a large demand for such services induced cybercriminals to create this market, or has supply awakened interest and attracted a large number of perpetrators? The answer is probably a bit of both. This does indeed appear to be a vicious circle.

To understand the underlying dynamics, it is first necessary to examine why cyber extortion was inherently predestined to gain great popularity among a wide range of perpetrators. Firstly, this type of attack can quickly be turned into large sums of money, as repeatedly discussed:[72] a bitcoin payment is sent directly from the victim to the perpetrator and is "laundered" using a bitcoin mixing service so that the flow of money can no longer be traced. Secondly, the search for targets is very easy, given the practically infinite supply of potential victims. This type of attack has also been discussed heavily in the media, and numerous victims and criminal success stories are known, but hardly any convictions. This gives perpetrators the impression that they can escape with impunity, which is a strong incentive: many perpetrators in real space, especially in the traditional petty criminal scene, try their luck in virtual space. As soon as there is demand, the market adjusts, offering a whole range of services that are as user-friendly as possible. This tailored range of services and its ready availability give even more of a boost to the market, allowing even more perpetrators to enter the business.

The actual problem of course consists in the suppliers of these products. But apparently there is only a limited number of them. According to the estimates of Andy Archibald, head of the UK National Crime Agency's cybercrime unit, there were no more than 100-200 individuals in 2015, but they had a substantial leveraging effect.[73] Because of the opening-up of the market and the large number of perpetrators and products, it is also very difficult to stay on top of these cybercriminal activities. This also makes the work of law enforcement authorities much more difficult.

6.2 Future design of two-factor and multi-factor authentication

The US National Institute of Standards and Technology (NIST) announced in July 2016[74] that its future guidelines on digital identities would no longer recommend authentication by text message, and would even recommend against it. While many places are still trying to get internet users to use two-factor authentication consistently, the suitability of text messages – the most popular and easy-to-use second factor – is already being disputed.

To log in securely to an internet service such as ebanking, a second authentication method is generally used alongside the password. Ideally, this second authentication is performed via a second, independent communication channel, often a mobile phone by text message. Because most mobile phones today are smartphones and thus small computers, they may be infected with malware that can intercept messages and forward them to the scammer. More-

[72] Transition from criminal activity to the reception of a laundered sum of money that can be used directly

[73] https://www.connectinternetsolutions.com/cyber-crime/ (as at 28 February 2017)

[74] https://pages.nist.gov/800-63-3/sp800-63b.html (as at 28 February 2017)

over, many banking transactions are now often conducted via smartphone, with the result that login and the second authentication are performed on the same device. This cancels out the additional security that one-time passwords by text message were intended to ensure.

But not only unsecured end-user devices are a threat to text messages as a second factor: also at the network level, this information can be tapped or redirected. Already years ago, security researchers pointed out the security problems of the SS7 protocol,[75] one function of which is to allow roaming between different mobile communication providers. Mobile phones can register with foreign networks abroad; the foreign network operator notifies the home network of the subscriber, which then forwards phone calls and text messages for delivery on the foreign network. This process can be faked even if the mobile phone is not located abroad. The text messages are then redirected to network operators abroad and can be intercepted there. This works because the underlying SS7 protocol was originally designed to be open. It operated under the assumption of basic trust among all mobile telecommunications providers. With the growing number of providers all around the world, however, the possibility is now greater that individual companies do not follow the rules and may fail to prevent fraudulent activities, or even work together with scammers.

On the non-technical side, cases using social engineering are possible. In one specific case, helpful telecom customer service employees were convinced by scammers to send a replacement SIM card to an address accessible to the criminals,[76] consequently allowing them to take over several online accounts.

Multi-factor authentication is based on at least two components. These components may be knowledge (e.g. a password), possession (e.g. a key card), or a unique characteristic (e.g. a fingerprint). Because of the increasing fusion of phone and computer as well as the integration of communication networks, mobile communication networks can no longer be seen as a separate communication channel independent of the internet. So text messages meet the "possession" criterion only in a limited way. Accordingly, if possible, online services – especially services with potential dameage – should switch to other authentication methods. If applied properly, an example of a secure authentication method based on a mobile phone consists in smartphone applications, that decode a one-time password encrypted by the service provider. Another alternative is the Mobile ID system, with which the authentication characteristics are already encrypted on the SIM card. Because services are increasingly used on smartphones themselves, the recommended additional factors for authentication are elements independent of the smartphone, such as separate hardware security keys, the use of which is already offered by many major web services.[77]

[75] https://www.blackhat.com/presentations/bh-europe-07/Langlois/Presentation/bh-eu-07-langlois-ppt-apr19.pdf (as at 28 February 2017)

[76] http://www.forbes.com/sites/laurashin/2016/12/20/hackers-have-stolen-millions-of-dollars-in-bitcoin-using-only-phone-numbers/#42981a5c22db (as at 28 February 2017)

[77] http://fc16.ifca.ai/preproceedings/25_Lang.pdf (as at 28 February 2017)

Conclusion:

But if your online service still uses text messages for authentication or password reset, you don't have to panic. Although this method meanwhile has several vulnerabilities and is no longer the most secure option, the use of two or more factors is still many times more secure than protection relying only on username and password.

6.3 Security technologies under constant pressure

To enhance security, the usual security products – such as antivirus scanners, micro virtualisation approaches and host intrusion detection/prevention systems – are frequently supplemented by standard Windows applications like AppLocker and EMET.[78] These two programs substantially enhance the security of Windows systems. With the help of AppLocker, it can be defined precisely in which folder which program should be executed, creating a major hurdle for attackers wanting to perform an initial infection. On the other side, EMET makes it more difficult to execute exploits.

Of course, malware programmers try to circumvent these protection tools. While this fact is not a new insight and has been described repeatedly,[79,80] a significant increase in such attacks has been observed since last autumn. For instance, attackers have been embedding macro code in Office documents containing a PowerShell script. The attacker is exploiting the fact that PowerShell scripts are permitted in most environments. Other approaches use regsvr32 and Scriptlets to achieve the same objective. The Angler exploit kit now also has the capacity to launch exploits in a way that the protective effect of EMET is circumvented: the attackers call memory allocation routines that belong directly to the attacked programs (e.g. Flash).[81]

Conclusion/recommendation:

The new protection technologies are used with increasing frequency and are effective against many of the existing attack vectors. But attackers are able and willing to look for (and find) a new way to circumvent any new security mechanism. Nevertheless, the use of these protection mechanisms still makes sense, as they increase the burden on attackers and continue to make a large number of currently popular attack vectors unusable. But we do recommend keeping a close eye on the possibilities that PowerShell offers for attackers and, for instance, introducing appropriate security measures such as digital signing of all scripts and macros. There are also various behaviour blocking engines that are at least partially able to detect such attacks. Microsoft has also implemented additional functions in DeviceGuard in Windows 10, creating further obstacles for attackers.

[78] The Microsoft Enhanced Mitigation Experience Toolkit (EMET) includes the functions Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP), among others

[79] http://subt0x10.blogspot.ch/2016/04/bypass-application-whitelisting-script.html (as at 28 February 2017)

[80] http://leastprivilege.blogspot.ch/2013/04/bypass-applocker-by-loading-dlls-from.html (as at 28 February 2017)

[81] https://www.fireeye.com/blog/threat-research/2016/06/angler_exploit_kite.html (as at 28 February 2017)

7 Politics, research, policy

7.1 Switzerland: parliamentary procedural requests

Item	Number	Title	Submitted by	Submission date	Council	Office	Deliberation status and link
Ip	16.4115	E-ID. Electronic identity	Rosmarie Quadranti	16.12.2016	NC	FDJP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164115
Mo	16.4089	Strengthening security policy instruments abroad	Damian Müller	15.12.2016	CS	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164089
Po	16.4073	Cyber risks. For comprehensive, independent, and effective protection	Roger Golay	15.12.2016	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164073
Po	16.3706	Digital economy and labour market	Beat Vonlanthen	27.09.2016	CS	EAER	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163706
Ip	16.3694	Are we in shape for working world 4.0?	Stefan Müller-Altermatt	22.09.2016	NC	EAER	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163694
Ip	16.4161	Julian Assange – a defender of human rights who should be protected?	Jean-Luc Addor	16.12.2016	NC	FDFA	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164161
Ip	16.4131	How can Switzerland take part in artificial intelligence research so that universal moral values are well-represented in the digital world?	Claude Béglé	16.12.2016	NC	EAER	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164131
Ip	16.4012	Dual education. How do we stay a world leader?	Claude Béglé	14.12.2016	NC	EAER	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164012
Ip	16.4001	Airbnb and co. Is liability governed by the rules of the internet platform or Swiss law?	Carlo Sommaruga	14.12.2016	NC	FDJP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164001
Ip	16.3960	Adjustment of our education system to the new world shaped by digitalisation	Claude Béglé	08.12.2016	NC	EAER	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163960
Po	16.3914	How can ethics be incorporated into algorithms?	Claude Béglé	28.11.2016	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163914
Mo	16.3902	Prohibition of adhesion contracts of online booking platforms against the hotel industry	Pirmin Bischof	30.09.2016	CS	EATC-CS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163902
Ip	16.3861	Formation of a digital Switzerland expert group	Fathi Derder	30.09.2016	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163861
Ip	16.3837	Civilian drones. Better protection for critical infrastructure	Manuel Tornare	30.09.2016	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163837
Ip	16.3829	Federal cybersecurity unit and darknet	Christian Imark	29.09.2016	NC	FDJP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163829

Qu	16.1058	Development of the advertising market. Outflow of money abroad and media financing	Jacqueline Badran	28.09.2016	NC	FDJP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20161058
Ip	16.4003	Digitalisation. Not jeopardising Switzerland as a data location	Marcel Dobler	14.12.2016	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164003
Ip	16.4002	Transport perspectives 2040. Where is digitalisation in the reference scenario?	Thierry Burkart	14.12.2016	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164002
Po	16.3918	Digital revolution. How can offliners be integrated?	Claude Béglé	29.11.2016	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163918
Po	16.3789	Digitalisation in public transport. Challenges relating to data protection	Evi Allemann	29.09.2016	NC		https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163789
Qu	16.1059	Terrorist attacks. Security of nuclear power plants?	Balthasar Glättli	28.09.2016	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20161059
Ip	16.4050	Digitalisation of the Swiss customs system. Reducing administrative burden	Viola Amherd	15.12.2016	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164050
Po	16.4078	Digitalisation. Making paperless e-voting possible	Marcel Dobler	15.12.2018	NC	FCh	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164078
Mo	16.4011	Digitalisation. No duplication of data gathering	Daniela Schneeberger	14.12.2016	NC	FDHA	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164011
Qu	16.5429	Tisa information leak. Attacks on data protection, net neutrality, and open source software	Balthasar Glättli	21.09.2016	NC	EAER	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20165429

7.2 Digital Switzerland strategy

In 2016, the Federal Council adopted the digital Switzerland strategy. This strategy supersedes the Federal Council's 2012 strategy for an information society in Switzerland.

Following the approach of a "free, open and secure" internet, the paper defines the strategic goals for the "free and open" aspect of the internet for Switzerland.

The national strategy for the protection of Switzerland against cyber risks (NCS), in contrast, focuses on the "secure" aspect of the internet, defining the strategic goals relating to security, trust, reliability and resilience for Switzerland.

At the heart of the digital Switzerland strategy is the consistent utilisation of the opportunities of digitalisation so that Switzerland can position itself as an attractive place to live and as an innovative, future-oriented location for business and research. The key objectives pursued by the Federal Council under this strategy are innovation, growth and prosperity in the digital world; equal opportunities and the participation of all; transparency and security; and contribution to sustainable development. The Federal Council defines the principles according to which the digital transformation should occur.

7.3 Swiss participation in the Cyber Europe 2016 exercise

Held for the fourth time, Cyber Europe has now become one of the largest and most comprehensive cyber exercises in the world. The biennial exercise is organised by ENISA, focusing on both the technical and operational aspects of a cyber crisis. 29 EU member states and EFTA countries, including Switzerland, took part last year. The first technical part already began in April 2016, allowing employees in the cybersecurity field to analyse complex, innovative and realistic technical incidents on a wide variety of topics. On 13 and 14 October, the operational part followed, in which experts participated from more than 300 organisations, including in the fields of telecommunications, cloud service providers, cybersecurity software and service providers, cybersecurity divisions, ministries and EU institutions. Cyber Europe 2016 dealt with topics such as the internet of things, drones, cloud computing, mobile malware and ransomware. For the first time, the entire scenario was supplemented by actors, journalists, simulated companies and social media in order to take adequate account of the aspect of public affairs. The Cyber Europe motto, "stronger together", expresses that cooperation at all levels is the key to successfully dealing with major cross-border cyber incidents.

8 Published MELANI products

In addition to the semi-annual reports for the general public, MELANI also offers a number of diverse products. The following sections provide an overview of the blogs, newsletters, checklists, instructions and fact sheets drawn up during the reporting period.

8.1 GovCERT.ch blog

8.1.1 Tofsee spambot features .ch DGA – reversal and countermeasures

22.12.2016 – The malware which MELANI / GovCERT identified as Tofsee tried to spam out hundreds of emails within a couple of minutes. However, this wasn't the reason why it popped up on the radar. The domains queried by the malware explain why this particular sample caught our attention. The domains appear to be algorithmically generated, and about half of the domains use the country code top level domain (ccTLD) of Switzerland.

➔ https://www.govcert.admin.ch/blog/26/tofsee-spambot-features-.ch-dga-reversal-and-countermesaures

8.1.2 When Mirai meets Ranbyus

15.12.2016 – Over the past few weeks, MELANI / GovCERT has seen a rise in malicious Microsoft Office documents that are being spammed out to Swiss internet users with the aim of infecting them with a malicious software (malware) called Dridex. Dridex is an ebanking Trojan which has already been around for some time now.

➔ https://www.govcert.admin.ch/blog/23/dridex-targeting-swiss-internet-users

8.1.1 SMS spam run targeting Android users in Switzerland

13.07.2016 – MELANI / GovCERT.ch received several reports today about malicious text messages sent to Swiss mobile numbers. The text messages are written in German and claim to come from the Swiss Post. But in actual fact, the messages were sent by hackers with the aim of infecting smartphones in Switzerland with a Trojan horse.

➔ https://www.govcert.admin.ch/blog/24/sms-spam-run-targeting-android-users-in-switzerland

8.1.2 Dridex targeting Swiss internet users

08.07.2016 – Over the past few weeks, MELANI / GovCERT has seen a rise of malicious Microsoft Office documents that are being spammed out to Swiss internet users with the aim of infecting them with a malicious software (malware) called Dridex. Dridex is an ebanking Trojan which has already been around for some time now. The attackers are operating various botnets with Dridex-infected computers. While most of these botnets have a strong focus on financial institutions from abroad (such as US or UK), one particular botnet is also targeting financial institutions in Switzerland.

➔ https://www.govcert.admin.ch/blog/23/dridex-targeting-swiss-internet-users

8.2 MELANI newsletter

MELANI published the following newsletters in the second half of 2016:

8.2.1 Social engineering: new attack method directed against companies

20.01.2017 – In recent days, the Reporting and Analysis Centre for Information Assurance MELANI received reports of several cases in which scammers called companies, pretending to be a bank, and claimed that an ebanking update had to be carried out the following day. They requested several employees of the finance department to be available on that day. The purpose of this was to circumvent the security element of a joint signature and in that way to release a fraudulent payment.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/social-engineering--neue-angriffsmethode-richtet-sich-gegen-firmen.html

8.2.2 Ebanking: attackers targeting mobile authentication methods

29.11.2016 – Over the past few weeks, MELANI received reports of several cases in which hackers succeeded in using social engineering to trick victims into authorising fraudulent payments in ebanking.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/mobileauthentifizierungsmethoden.html

8.2.3 Cyber extortion: key topic in MELANI semi-annual report

26.10.2016 – The 23rd semi-annual report of the Reporting and Analysis Centre for Information Assurance (MELANI), published today, highlights the main national and international cyber incidents of the first half of 2016. The report analyses the key topic of increased numbers of attacks using cyber extortion. It also focuses on various data leaks.

➔ https://www.melani.admin.ch/melani/en/home/dokumentation/newsletter/semi-annual-report-2016-1.html

8.2.4 Offline payment software targeted by hackers – Swiss companies affected

25.07.2016 – Over the past few days, MELANI has observed several cases of the Dridex malware targeting offline payment software solutions. This kind of software is generally used by companies to transmit a large number of payments to one or more banks online. If computers using such software are compromised, the potential damage can thus be massive. MELANI urgently recommends that companies protect computers used for payment transactions accordingly.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/offline-payment-software.html

8.2.5 Increasing circulation of malicious Office documents

08.07.2016 – In recent weeks, the Reporting and Analysis Centre for Information Assurance MELANI received numerous reports about malicious Microsoft Office documents spread by email with the aim of infecting the victim's computer with malware. MELANI thus expressly warns against opening such Office documents and recommends that internet users exercise greater vigilance when using Office documents and not to execute Office macros.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/malicious_office_documents.html

8.3 Checklists and instructions

In the second half of 2016, MELANI did not publish any new checklists or instructions.

9 Glossary

Term	Definition
Accessibility service	An accessibility service is an application making a user interface available to support users with disabilities or users who are no longer fully able to interact with their device.
Advanced persistent threats (APTs)	This threat results in very significant damage impacting an individual organisation or a country. Attackers are willing to invest a great deal of time, money and knowledge in the attack and generally have considerable resources at their disposal.
App	"App" (an abbreviation of "application") generally refers to any type of application program. In common parlance, the term now commonly refers to applications for modern smartphones and tablet computers.
Backdoor	"Backdoor" refers to a software feature that allows users to circumvent the usual access control of a computer or of a protected function of a computer program.
Backup	"Backup" means the copying of data with the intent of copying it back in the event of data loss.
Barcode	A "barcode" is an imprint that can be read optoelectronically and that consists of parallel lines and gaps of differing width.

Bitcoin	Bitcoin is a decentralised payment system that can be used worldwide, as well as the name of a digital monetary unit.
Booter/Stresser	Tools triggering DDoS attacks in return for payment ("DDoS as a service").
Browser	Computer programs that are mainly used to display diverse content in Web pages. The most well-known browsers are Internet Explorer, Opera, Firefox and Safari.
Brute force	Brute force is a method for solving problems in the fields of computer science, cryptology, and game theory based on trying out all possible cases.
Bundle identifier	A bundle identifier is an expression for identification which is defined when developing an app and subsequently maintained, usually in the form of com.yourcompany.app-name.
Command & control server	Most bots can be monitored by a botmaster and receive commands via a communication channel. This channel is called a command & control server.
Cookies	Small text files stored by a web page when viewed on the user's computer. For example, user preferences for a website can be stored with the assistance of cookies. However, cookies can also be abused to compile an extended user profile about one's surfing habits.
DDoS	Distributed denial of service attack. A DoS, or denial of service, attack where the victim is simultaneously attacked by many different systems.
Defacement	Unauthorised alteration of websites.
Domain generation algorithm	Domain generation algorithms are used by numerous malware families in order to periodically generate a large number of domain names, which are then used as contact points to command & control servers.
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).

Fast flux	Fast flux is a DNS technique used by botnets to hide the location of webservers.
E-currency services	A monetary value in the form of a receivable from the issuing authority. The value is saved on a data carrier, issued in return for a sum of money – the value of which is not less than the issued monetary value – and accepted by companies other than the issuing authority as a means of payment.
Ethernet	Ethernet is a technology for wired data networks.
Google rank	The PageRank algorithm is a procedure for evaluating and weighting a set of linked documents, such as the World Wide Web, according to its structure.
Grey hat	Grey hats may break laws or restrictive interpretations of hacker ethics, but with the purpose of achieving an ethical objective.
Hacker ethics	"Hacker ethics" refers to a collection of ethical values that are said to be crucial to hacker culture. Key values include freedom, cooperation, voluntary and self-chosen work, and sharing.
ICANN	Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit organisation under private law with headquarters in the Los Angeles neighbourhood of Playa Vista. ICANN decides on the foundations for administering top-level domains. In this way, ICANN coordinates technical aspects of the internet without, however, using binding law.
Industrial control systems (ICSs)	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.
JavaScript	Is an object-based scripting language for developing applications. JavaScripts are program components integrated in HTML code enabling specific functions in internet browsers. For example, while checking user input on an internet form, a JavaScript can verify that all the characters entered of a telephone number are actually numbers. As is the case with ActiveX Controls, JavaScripts are run on the computer of the website visitor. Aside from useful features, unfortunately dangerous

	functions can also be programmed. In contrast to ActiveX, JavaScript is supported by all browsers.
Malware	Generic term for software which carries out harmful functions on a computer, e.g. viruses, worms, Trojan horses.
mobileTAN	mobileTAN is a way to incorporate text messages (SMSs) as a transmission channel. After online banking clients transmit their completed funds transfer requests on the internet, the bank sends them a text message on their mobile phone with a TAN that can be used only for that transaction.
Offline payment software	Payment entry software installed locally.
Phishing	Fraudsters phish in order to gain confidential data from unsuspecting internet users. For example, this can be account information from online auctioneers (e.g. eBay) or access data for online banking. The fraudsters take advantage of their victims' good faith and helpfulness by sending them emails with false sender addresses.
Plain text	"Plain text" refers to data that can be implemented directly using a character code.
Plug-in	A plug-in is an optional software module that extends or changes existing software.
Port scanner	A port scanner is software used to check which services a system working with TCP or UDP offers via the internet protocol.
PowerShell script	PowerShell is a cross-platform framework by Microsoft for automating, configuring, and administering systems, consisting of a command line interpreter and a scripting language.
Proxy	A proxy is a communication interface in a network. It works as a mediator, receiving queries on the one side and making a connection on the other side via its own address.

QR code	A QR code (Quick Response Code) consists of a square matrix made up of black and white squares representing binary coded data.
RFID code	"RFID" refers to a technology for transmitter-receiver systems for the automatic and contactless identification and localisation of objects and living things using radio waves.
Router	Computer network, telecommunication, or also internet devices used to link or separate several networks. Routers are used in home networks, for instance, establishing the connection between the internal network and the internet.
Malicious code	Generic term for software which carries out harmful functions on a computer, e.g. viruses, worms, Trojan horses.
Vulnerability	A loophole or bug in hardware or software through which attackers can access a system.
SHA	The term "secure hash algorithm" (SHA) refers to a group of standardised crypto logical hash functions.
SIM card	A SIM card (subscriber identity module) is a chip card inserted into mobile phones and used to identify the user on the network.
Smartphone	A smartphone is a mobile phone that offers more computer functionality and connectivity than a standard advanced mobile phone.
SMS	Short Message Service for sending text messages (160 characters maximum) to mobile phone users.
SQL injection	SQL injection refers to the exploitation of a vulnerability in connection with SQL databases, resulting from insufficient verification of the variables to be transmitted. The attacker attempts to inject his own database commands in order to change the data as desired or to gain control over the server.

SS7	Signalling System No. 7 (SS7) is a collection of protocols and procedures for signalling in telecommunication networks. It is often used in the public telephone network, in connection with ISDN, landline and mobile communication networks, and since about 2000 also more frequently in VoIP networks.
Take-down	Expression used when a provider takes down a site from the network due to its fraudulent content.
USB	Universal Serial Bus (with a corresponding interface) which enables peripheral devices such as a keyboard, mouse, external data carrier, printer, etc. to be connected. The computer does not have to be switched off when a USB device is unplugged or plugged in. For the most part, new devices are automatically identified and configured (depending on the operating system).
Encryption Trojans/ 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.
Web browser	Computer programs that are mainly used to display diverse content in Web pages. The most well-known browsers are Internet Explorer, Firefox and Safari.
WLAN	WLAN stands for Wireless Local Area Network.
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.)