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 2017/I (January – June)

2 NOVEMBER 2017

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

1 Overview / Content

2 Editorial

Michel Buri
Deputy CIO
CISO
Valais Hospital

Dear reader,

The major global malware infection WannaCry which happened on 12 May 2017 will be hard to forget. Numerous private and public companies suffered serious damage with the UK National Health Service being particularly badly hit. We have probably all asked ourselves the question "What if...?". As we all know, we escaped relatively unscathed considering that the consequences could have been completely disastrous. Everyone has surely asked themselves the more fundamental question of whether the balance between risk and benefit in IT has always been properly judged and whether the residual risk is still acceptable.

This question is a major preoccupation for hospitals today. Medicine in the 21st century means closer patient involvement during the treatment process. It will depend heavily on these technologies and medical treatment will increasingly involve the use of connected medical devices. At the same time, the prospect of cyber attacks like WannaCry represents enormous institutional challenges (e.g. patients' physical integrity or the inability to ensure the continuity of activities).

An initial response to the question of whether the risk is acceptable was provided by doctors in an article in the New England Journal of Medicine on 7 June 2017 in which they wrote "*We wouldn't accept being told to use outdated equipment on our patients, and our now-critical IT should be no different*"[1]. Just as we should never use an expired syringe or medication, neither should we should we be using connected medical appliances which run on antiquated operating systems or which are not equipped with the latest safety updates. And yet this is exactly what happens at the moment.

This is one of the biggest challenges facing today's health care sector. We should approach cyber security in a dynamic and holistic manner in order to guarantee the proper operational security of connected medical devices for the entire duration of their lifetime.

In order to tackle this problem, all leaders and parties involved need to work closely together, this includes manufacturers, hospitals and the Swissmedic regulatory authority. MELANI plays a key role as facilitator in this ecosystem which is dedicated to connected medical device safety.

I hope you enjoy reading this new report.

Michel Buri

[1] R. Clarke, T. Youngstein. Cyberattack on Britain's National Health Service – A wake-up Call for Modern Medicine. In NEJM, June 2017 (as at 31 July 2017).

3 Key topic: WannaCry and NotPetya - encryption software or more?

In the first half of 2017, two events made the headlines worldwide in the cyber domain. On 12 May 2017, the WannaCry encryption Trojan attacked at least 200,000 computers in 150 countries according to information from Europol. Those affected included the Spanish telecommunications service provider Telefonica, hospitals in the UK and Deutsche Bahn. MELANI was able to identify potential 204 victims in Switzerland, although in comparison to foreign countries, no operator of critical infrastructures was affected. On 27 June 2017, the malware NotPetya caused a great deal of damage above all in Ukraine. Those affected included Kiev airport, the National Bank of Ukraine and the radioactivity measuring station in Tschernobyl. However, other countries were also affected, e.g. the Danish shipping company Maersk, the biggest container shipping company in the world and the US pharmaceutical company Merck. In Switzerland, the Admeira advertising company among others fell victim to NotPetya. What specific features both of these attacks exhibit and what issues they raise will be dealt with in the following chapters.

In the case of attacks using ransomware, data on the victim's computer is encrypted. The victim is subsequently asked to pay a ransom so that the data can be restored. Encryption software of this nature has already been in use for a relatively long period of time. Nonetheless, for some time now more and more criminals seem to be resorting to using this type of malware. MELANI is closely monitoring developments in this area and has already highlighted many times before in past semi-annual reports the different types and approaches.[2] Moreover, on 19 May 2016, MELANI carried out a ransomware awareness day with numerous partners on the topic of ransomware.[3] These incidents show once again how vulnerable modern society is with its networked computer systems.

Recommendation:

INFO

MELANI information page on encryption Trojans
https://www.melani.admin.ch/melani/en/home/themen/Ransomware.html

3.1 Procedure

In both cases a vulnerability in the SMB protocol was misused to spread the malware. SMB is a network protocol for file, printing and other server services and is the core of Microsoft's network services. Furthermore, SMB is used by the freely available software project "Samba" to allow Windows systems to access resources of Unix-based systems and vice versa.

The attacks were preceded by the publication of a hacking tool with the name "DoublePulsar" by the Shadow Broker group in April 2017. This hacking tool also took advantage of the

[2] https://www.melani.admin.ch/melani/en/home/themen/Ransomware.html (as at 31 July 2017).
[3] https://www.melani.admin.ch/melani/en/home/dokumentation/newsletter/ransomwareday.html (as at 19 May 2016).

aforementioned SMB vulnerability "Eternal Blue". "DoublePulsar" is a backdoor implant tool, which was presumably developed and used by the US National Security Agency (NSA). It was assumed that DoublePulsar had been stolen together with other tools from the US authorities already in 2016.

In the case of WannaCry, the infection had very probably occurred via drives visible over the internet with outdated SMB software because up to now there is no indication of other infection paths such as emails, for example. By contrast in the case of NotPetya, a manipulated update of an accountancy software called MeDoc was identified as the initial vector. Companies operating in Ukraine must use this software to pay taxes. If a computer in a company network was infected, the SMB loophole made it possible for NotPetya to be able to laterally move around the corresponding company network. In addition, the attackers have integrated other alternative possibilities for lateral dissemination. The cases differ from each other to the extent that, in the case of WannaCry, the attackers took a chance on placing their software, whereas in the case of NotPetya, it is reasonable to assume that targeted Ukrainian companies were to be attacked.

In view of the potential of both attacks, the handling of the ransom payments must be described as unprofessional: in the case of NotPetya, the attackers used email communication. The corresponding email address was swiftly blocked, however, which made communication with the victims impossible and also prevented a decryption code being sent to the victims. This information was quickly reported in the media which is why only a few victims paid. In addition, the ransom demanded amounting to just over USD 300 was comparatively small in both cases.

3.2 Criminal background or targeted sabotage?

In both cases, the security experts called a purely criminal background into question. The unprofessional implementation of the payment components underscored the doubts that in both cases the focus was indeed on financial interests. The goal of ransom seekers whose motivation is purely financial is to blackmail a high overall amount from their victims as quickly and efficiently as possible. As a result it is this part of the attack process that experience shows is the most well thought out, which cannot be said of WannaCry and NotPetya.

According to experts, there were similarities between the malicious code of WannaCry and the malware Lazarus which was used in the attack on the Central Bank of Bangladesh in March 2016. In the case of NotPetya, there are signs that the targeted dissemination vector via the Ukrainian accounting program MeDoc means that sabotage is likely to have been the main motivation of the perpetrators. That companies outside Ukraine were also affected is probably related to the fact that these companies operate in Ukraine and accordingly must use this accountancy software. Who is behind both attacks will probably never be fully clarified. The case thus shows in an exemplary way the advantages of a cyber attack: as is usual in such cases, all that remains are clues. There is no hard evidence. While everybody speculates on the motivation and origin of the attack, the attacker can hide behind the anonymity of the internet.

3.3 The problem of systems which are not updated

The propagation of the malware was successful in both cases because the associated security vulnerability in the SMB protocol permitted dissemination without user interaction. At this

point in time, the vulnerability had been known, however. Microsoft had published an update already at the start of March 2017. Correspondingly, an incident such as WannaCry or NotPetya should never have led to infections. Why in spite of this were well-known companies victims of these attacks? On computers which are in private use, updates are often downloaded with an automatic update function. When a manufacturer publishes updates on a Tuesday, these will already have been installed on the Wednesday on a large number of private computers. However, in the business sector, the situation is different. Here updates cannot simply be downloaded overnight. A faulty update can lead to a business-critical application no longer working and a company can post losses because of this. This is why tests must firstly be carried out to ensure that the updates made available by the software companies will not have any negative effect on business-critical applications. An assessment must therefore be carried out before each update as to whether the risk of an update which has not been downloaded exceeds that of a non-functioning application. Other risk-reducing measures can also of course be implemented such as the isolation of endangered systems.

In certain areas, an update is often even virtually impossible, for example in the healthcare field. With each change such as downloading an update, medical appliances would lose their certification and thereby their authorisation. The risk would thus be passed from the manufacturer to the operator. A faulty update in a medical appliance can possibly have life-threatening consequences. It is thus understandable that hospitals, medical practices, laboratories, etc. do not want to take this risk. A recertification would remove the problem. However, a recertification leads to excessive costs, requires time and is also not possible everywhere. That in the case of WannaCry with its untargeted, global spread even the healthcare field was affected is not surprising viewed from this perspective.

3.4 The responsibility of security services

To respond adequately to the increased challenges in the fields of security, security services such as the police or intelligence services have to increasingly use electronic methods to monitor target persons. Because internet communication is increasingly being encrypted, the focus is on the terminal devices of the targeted persons to gather information before it is transmitted encrypted. This is why unknown vulnerabilities (zero-day vulnerabilities) are a means to an end for security services. If the devices of a target have the latest standard of technology and people do not allow themselves to be cheated by social engineering, this is one of the only possibilities to get into the target system. But the use and withholding of knowledge about vulnerabilities undermines the process of responsible disclosure. In line with this, this knowledge is always linked to great responsibility and requires regulated, documented and controlled risk management, especially on the part of the government.

It may be concluded that governments primarily use zero-day vulnerabilities with the focus on a specific target. But that is not true for other actors. If vulnerabilities of this nature are made public suddenly and in an uncontrolled manner and used irresponsibly by a third party, the damage caused can be greater than the expected added value of the security service. This has been shown by the WannaCry and NotPetya cases. The knowledge of the vulnerability in the SMB protocol and the associated tools which simplified taking advantage of the vulnerability, came apparently from the NSA group. The information was made public by the Shadow Broker group in mid-April 2017. But the group already claimed to have stolen zero-days information from the NSA in August 2016.

If the vulnerability and the corresponding exploit which was used by WannaCry and NotPetya really came from an intelligence service which lost this knowledge to third parties already in 2016, swift information to Microsoft and corresponding provision of a patch could have prevented things from getting worse. It is questionable that notice was given at all because of the late publication of the patch. If there was no notification and no responsible disclosure to Microsoft, even after the knowledge of the loss and the severity of the vulnerability, the risk of an uncontrolled publication of critical security holes would have been taken into account.

There were already cases in the past where information about zero-day vulnerabilities were stolen and subsequently misused for criminal purposes: In 2015 Hacking Team was the victim of a hacker attack. The data stolen was subsequently published on the internet. "Vault 7" is a series of documents which Wikileaks published from 7 March 2017. Among other things, they refer to 24 zero-day vulnerabilities in the Android operating system which the CIA apparently knew about in 2016.

3.5 Data backup – life insurance for every company

Whether and how much an insurance company finally pays out is known by only a few people but in spite of this, everyone hopes that the insurance company will fully cover any damage suffered. The frustration is immense if the damage is not covered by the policy, if the amount covered is too small or the insurance policy had not been paid. Everyone would be well advised from time to time to check their policy and if need be to make adjustments to meet changing circumstances. There is a similar behaviour in the field of data backup.

In a company, the data stored is the basis for daily business without which no money can be earned. It includes customer contacts, customer correspondence, orders, accounting, the website with any databases and much more data which are essential for daily operation. There is thus no doubt that this data must be regularly saved. However, one should not simply rely on the backup working. The backup function must be regularly tested. It also has to be regularly examined whether or not really all relevant data was taken into account in the back-up process.

In the case of loss of data, for example in connection with encryption Trojans another aspect is added. As a rule, the installation of back-up data lasts several hours. Employees are not able to work during this period. At best this results in a loss of profits, in the case of critical infrastructure such as hospitals this can, however, have far worse outcomes. In the case of WannaCry, hospitals in the UK had to shut down their emergency services and send patients to other hospitals.

Recommendation:

Define a backup strategy.

Consider which data and how often this has to be saved and how long the individual backups should be saved.

The backup should be stored offline, e.g. on an external medium such as an external hard disk, which is disconnected from the computer after the back-up procedure is complete, so that encryption Trojans have no access to this. Otherwise data on the back-up medium might also be encrypted and rendered unusable in the event of a ransomware attack.

4 Situation in Switzerland

4.1 Industrial control systems (ICSs)

Operators of critical infrastructures can also become victims of ransomware attacks, as described in section 3. However, ransomware rarely locks directly onto industrial control systems, instead it usually infects "administration systems". Nevertheless, interference with these "administration systems" can affect production.

Ransomware which specifically targets industrial control systems has so far only come to light in research work.[4] The Institute of Technology in Georgia (USA) described a scenario in which it was possible to encrypt the installed logic controller using the experimental LogicLocker and extort ransom money from operators.

In another case, a company named CRITIFENCE developed the Clear Energy[5] ransomware prototype in order to better market the measures to close the gaps in ICS products which CRITIFENCE had previously discovered. The malware blocks access to the logic controller and threatens to overwrite it and therefore renders it unusable. Luckily, these examples have not yet left the laboratory environment and have yet to make it into any production environments.

However conventional ransomware attacks on equipment which is used for the remote monitoring of ICS systems have already been recorded in Switzerland. A system which controls a water supply was attacked by ransomware. The malware spread across the remote monitoring system which could be accessed via the internet. This was most likely the result of a brute force attack on the relevant server. However, there were no serious consequences as it was possible to restore the system with the help of backups and then ensure it was secure. This is a perfect example of how each additional function, in this case the remote system monitoring, also requires additional safety measures.

Increasingly, sections of the central controls of industrial control systems are also outsourced to the cloud. Gornergrat Bahn railway[6], for example, uses a cloud-based virtual train traffic control system. The plan to introduce driverless trains in the future[7] means that the criticality of the control systems is even greater. Therefore, it is essential that these control systems are well protected.

---

4 http://www.cap.gatech.edu/plcransomware.pdf (as at 31 July 2017).

5 http://securityaffairs.co/wordpress/57731/malware/clearenergy-ransomware-scada.html (as at 31 July 2017).

6 https://www.siemens.com/innovation/en/home/pictures-of-the-future/mobility-and-motors/urban-mobility-gornergratbahn.html (as at 31 July 2017).

7 https://www.sob.ch/medienmitteilung/news/2017/6/15/sob-treibt-automatisches-fahren-voran.html (as at 31 July 2017).

Recommendation:

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

MELANI reporting form:

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

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

4.2 Attacks (DDoS, defacements, drive-bys)

Individuals, organisations and companies in Switzerland continue to be targeted by different kinds of attacks.

4.2.1 CERN has analyzed the VENOM Linux Rootkit

On 11 January 2017, the CERN Computer Security Team in Geneva published a worldwide warning about the VENOM rootkit[8]. A rootkit is a software tool which attackers install on a compromised system in order to conceal their logins and hide their processes and data. In the case of VENOM the attacker loaded the malware in automated form onto the file system and changes were made within a matter of minutes. During this process, the system time was manipulated so that files included incorrect modification time stamps which meant the changes could not easily be discovered. Whenever possible, the malicious code was ran directly on the computer under attack from its temporary memory (RAM). This was to avoid leaving any traces on the drives. The malware targets Linux servers and installs a backdoor on the affected device. It can execute commands and modify files remotely. The EGI CSIRT[9] suspected the initial infection was made remotely via SSH using stolen access data. The attack showed similarities to the intrusion to the Freenode[10] Chat-Server in 2014. The VENOM rootkit has targeted at the community of astrophysics. At the CERN there were no implications observed.

[8] https://security.web.cern.ch/security/venom.shtml (as at 31 July 2017).

[9] https://wiki.egi.eu/w/images/c/ce/Report-venom.pdf (as at 31 July 2017).

[10] https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2014/october/analysis-of-the-linux-backdoor-used-in-freenode-irc-network-compromise/ (as at 31 July 2017).

Recommendation:

As Venom does not leave any traces behind on the infected device, a log memory system is recommended so that any such cases can be analysed at a later date.

4.2.2 Propaganda instead of water temperature

Increasingly, political tensions are expressed digitally. Whereas graffiti used to be sprayed across the walls of buildings, nowadays hacktivists deface websites. For attackers, the advantage of digital devastation is that they do not need to be physically present and can instead spread their propaganda from anywhere in the world. This separation from local presence means that international events can also have an impact on Swiss websites.

At the end of May 2017, activists at a demonstration in Bern carried a banner saying "Kill Erdogan with his own weapons" through the streets. In the days that followed, MELANI recorded numerous so-called "defacement attacks" on Swiss websites[11]. This meant that, for example, visitors to the website of the Wülfingen lido were confronted with Turkish nationalist messages rather than the water temperatures they were actually looking for.

Figure 1: Defaced website of Wülflingen lido

It was a complete coincidence that a lido, in particular this one, was affected. Hacktivists look for websites with vulnerabilities. Attackers would doubtlessly like to place their messages on the high-traffic websites of well-known companies and organisations. However, these are often well protected, which is why the attackers often turn to smaller websites.

It was not only Swiss websites which were misused for this propaganda. Hacked Twitter accounts[12] were also used as a method of distribution. Their repertoire included other types of

[11] http://www.tagesanzeiger.ch/digital/internet/tuerkische-propaganda-auf-schweizer-badiwebsite/story/12947804 (only available in German) (as at 31 July 2017).

[12] https://www.theregister.co.uk/2017/03/15/twitter_app_hack/ (as at 31 July 2017).

attack: Turkish hackers confessed to DDoS attacks on the Austrian oe24.at website in March 2017[13].

Political propaganda does not have to be the only reason for defacements. As relevant portals[14] show, they are often a search for recognition or a competition between like-minded people.

Recommendation:

Attacks on content management systems (CMSs) used to create websites can be reduced dramatically by patching (prompt incorporation of security updates). However, several other measures can also contribute to the security of CMSs.

Measures to secure content management systems (CMSs)

https://www.melani.admin.ch/melani/en/home/dokumentation/checklists-and-instructions/measures-to-secure-content-management-systems--cms-.html

4.2.3 Online media still being misused as an infection channel

In its semi-annual report 2012/2[15], MELANI warned of the risks brought by the increasing inclusion of third-party content in websites. Media portals are often number one for including linked videos, advertising and social networks. At this point, MELANI reported visitor infections from such media portals on numerous occasions [16/17].

In spring 2017, Swiss news portals were attacked once again. In March, 20min.ch[18] reported that unauthorised parties had managed to access their online portal in order to place malicious scripts. A similar incident occurred again at pctipp.ch in April[19]. A smuggled script was used to try to redirect online readers to sites containing malware.

---

13 http://www.oe24.at/oesterreich/politik/Attacke-auf-oe24-Tuerkische-Hacker-bekennen-sich/273401472 (as at 31 July 2017).

14 http://zone-h.com/ (as at 31 July 2017).

15 cf. MELANI semi-annual report 2/2012, section 5.5 https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2012-2.html (as at 31 July 2017).

16 cf. MELANI semi-annual report 2/2015, section 4.3.1 https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2012-2.html (as at 31 July 2017).

17 cf. MELANI semi-annual report 1/2016, section 4.4.2 https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2012-2.html (as at 31 July 2017).

18 http://www.20min.ch/digital/news/story/Angriffsversuch-auf-20minuten-ch-vereitelt-27863282 (only available in German) (as at 31 July 2017).

19 http://www.pctipp.ch/in-eigener-sache/artikel/drive-by-angriff-auf-pctipp-87549/ (as at 31 July 2017).

Media portals are of interest to attackers because their high number of visitors means they reach a large range of potential targets. An example of this was the massive malvertising campaign ran by the group known as AdGholas[20]. With the help of so-called exploit kits, tailor-made malware is distributed to the victim.

The complete instructions and checklist can be found at www.melani.admin.ch :

DOCU

Measures to secure content management systems (CMS)

https://www.melani.admin.ch/melani/en/home/dokumentation/checklists-and-instructions/measures-to-secure-content-management-systems--cms-.html

In addition you will find instructions and a checklist here on what to do when an attack has already occurred:

DOCU

Instructions for cleaning up websites

https://www.melani.admin.ch/melani/en/home/dokumentation/checklists-and-instructions/instructions-for-cleaning-up-websites.html

4.2.4 Thank you for registering - user registration spam

Billions of unsolicited advertising emails, so-called spam, are sent globally on a daily basis. The spam filters used by email providers are improving all the time and mean that most users usually end up receiving a tolerable amount. However, at the beginning of 2017, MELANI recorded an increase in reports of unsolicited emails which were sent to specific individual recipients. Organisations and private individuals received numerous unsolicited emails requesting that they sign up for various newsletters, forum contributions and other similar services which required registration. If a programme automatically registers for such services, this is referred to as a so-called “subscription bomb".[21]

If no confirmation is required, the victims go on to receive all the subsequent follow-on messages from the various services. However, it is possible to unsubscribe from such services and set the relevant filters but dealing with many thousands of these registrations can require extensive effort from those affected.

---

20 https://www.proofpoint.com/us/threat-insight/post/massive-adgholas-malvertising-campaigns-use-steganography-and-file-whitelisting-to-hide-in-plain-sight (as at 31 July 2017).
https://www.proofpoint.com/us/threat-insight/post/adgholas-malvertising-campaign-using-astrum-ek-deliver-mole-ransomware (as at 31 July 2017).

21 http://www.forbes.com/sites/leemathews/2017/05/10/secure-email-provider-attacked-with-500k-newsletter-sign-ups/ (as at 31 July 2017).

4.3 Social Engineering and phishing

In addition to all the technical attacks, the most successful are those where attackers use credible stories in order to persuade victims to do as they wish. So-called "social engineering" attacks work best when the attacker can collate a lot of information on a potential victim. To do this, fraudsters use both freely available sources and information originating from data theft. Stolen data is analysed, coupled with other stolen or public data, prepared and sold on to other criminals. In the past, attackers used to content themselves with the contact list from an email account. They wrote to potential victims saying that the sender had lost their mobile telephone and wallet/purse and needed urgent financial assistance. Nowadays, criminals take the time to sift painstakingly though the emails in a compromised account looking for usable material. For instance, they look for electronic bills or invoices, edit the IBAN number and resend them to the victim. The fact that apparently unusable data is also exploited to commit fraud can be seen in the case in which the list of vendors from an exhibition was used as a source of information. Specific companies were written to and told that they had met the sender at the event. The email went on to explain that they had talked about a "big" deal which had to be dealt with with the utmost discretion. This is how they established a foundation of trust. The employers were then put under pressure and asked to pay a large sum of money.

4.3.1 Phishing

Numerous phishing emails were again sent out in the first half of 2017. The content of the emails did not differ greatly: some requested credit card data for "verification" purposes, while others directed the victim to linked pages requesting usernames and passwords for online services. Frequently, phishing emails also contain the logos of well-known companies or service in question in order to make the emails look official.

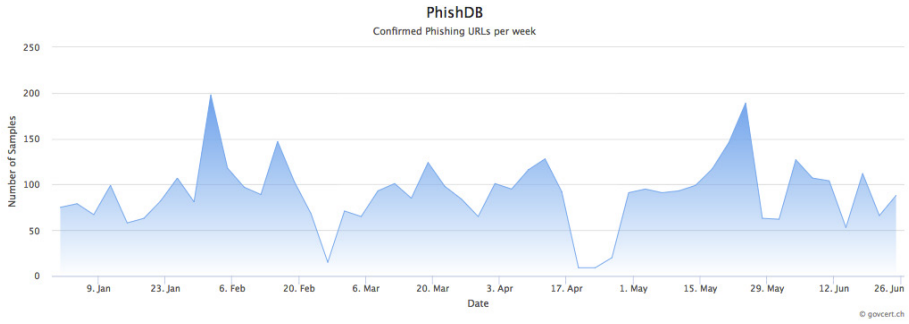

Figure 2: Reported and confirmed phishing sites per week on antiphishing.ch in the first half of 2017

Overall, 2343 different definite phishing sites were reported in the first half of 2017 using the antiphishing.ch portal operated by MELANI. Figure 2 presents the number of reported phishing websites per week. The number fluctuates over the half 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.

4.3.2 New attack method directed against companies

The first half of 2017 saw an increase in the number of telephone calls to potential victims (companies) where attackers pretended to be bank employees. This is easy for the attackers

as many companies publish their account details on their websites. The fraudsters can also obtain the information from a company in advance by telephone or email.

The caller pretends they have to carry out an e-banking update which then needs testing. However, in order to carry out the test, all the finance department employees need to be present, in particular those who are authorised to approve e-banking transactions. In order to generate trust, the fraudsters sometimes mention the names of existing employees.

In a second telephone call, a remote access tool has to be installed to which the caller needs access. They pretend that they want to check the system is working properly by making a test payment. As payments in the business world which exceed a certain amount require a joint signature in order to be processed, the fraudsters insist that those with signing powers provide their access data. In actual fact, they release the payment. In some cases, the attackers turn the victim's screen black so that they do not notice the fraudulent payment.

Recommendation:

This example shows how up-to-date social engineering methods still are. Awareness within individual companies is the key to effective protection from fraud attempts.

- Whenever possible, do not publish your bank details online
- Never allow unauthorised access to your system
- Never install so-called "remote tools" when requested to do so by third parties
- No bank will ever ask you to carry out any tests. Banks have their own IT departments or outsource their IT system. Security updates are always checked before they are made accessible to the public.

4.3.3 CEO Fraud - low-tech fraud

CEO fraud occurs when perpetrators instruct the accounting or finance department in the name of the CEO to make a payment to the (typically foreign) account of the scammers. Generally, the instruction is sent from a spoofed email address. But there have also been cases in which real compromised email addresses were used. The reasons given for the payment instruction differ, but the payment is usually claimed to be urgent and extremely sensitive (such as an acquisition). A consultant or a bogus or compromised law firm are also often part of the scenario. The attackers know exactly how they can use a supposedly urgent situation to put pressure on the employees in question so that they make the payment while circumventing any procedural requirements.

The fact that this type of fraud is growing at a tremendous rate confirms numerous statistics which were published in the first half of 2017. According to the German Federal Criminal Police Office (BKA), CEO fraud in the last few months has resulted in losses running into the millions.[22] In May of this year, the FBI also published figures on the huge increase in this type of fraud. It was found that CEO fraud between 2015 and December 2016 had increased by 2370%. According to the report, cases were reported in 132 countries with losses running into the billions.[23] The stolen funds are normally channelled to banks in China and Hong

[22] https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2017/CEO_Fraud_10072017.html (only available in German) (as at 31 July 2017).

[23] https://www.ic3.gov/media/2017/170504.aspx#fn3 (as at 31 July 2017).

Kong, although an increasing amount of money from this type of fraud is also routed to the United Kingdom. Social engineering attacks, which do not require any significant technical effort, have long been responsible for a considerable share of financial losses on the internet.

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.

Current threats: CEO fraud

https://www.melani.admin.ch/melani/en/home/themen/CEO-Fraud.html

Current threats: social engineering

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

4.3.4 Fake telephone support: increasingly sophisticated methods

For several years, scammers have been calling people in Switzerland. They usually pretend to be from Microsoft and make out that a computer problem requires troubleshooting via their telephone support. The fraudsters attempt to scare the victim by making them believe that their computer is damaged. They ask the victim to open the event viewer which shows all events and activities on the computer. Depending on the age and configuration of the computer, the list of error messages in the event log may be very long even though the system does not actually have any problems. The scammers attempt to access the computer with remote access software and then manipulate the system in order to request payment for the service allegedly provided. We have described this process on numerous previous occasions (the first time was in the Semi-annual report 2011/2, section 3.1)[24].

The telephone calls are still being made but the fraudsters are now using additional methods to make contact with their victims. One version still involves calling the victim but now a message is played when they answer the telephone. They are asked to call a particular telephone number in order to fix the problems which have supposedly been noticed on their computer.

Another more dangerous variant has been in operation abroad for some time and has recently appeared in Switzerland. It involves a pop-up window which appears when surfing the internet and stems from infected websites or adware installed on the computer. The pop-up contains a message, purportedly from Microsoft, which informs the reader that the computer has been infected with malware. The user is asked to call a number in order to avoid any sensitive data being stolen. As soon as they call the number, the standard fake telephone

[24] cf. MELANI semi-annual report 2/2011, section 3.1 https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2011-2.html (as at 31 July 2017).

support process continues, as described above. Interestingly, scammers sometimes use Swiss telephone numbers although calls to these numbers are most likely redirected abroad.

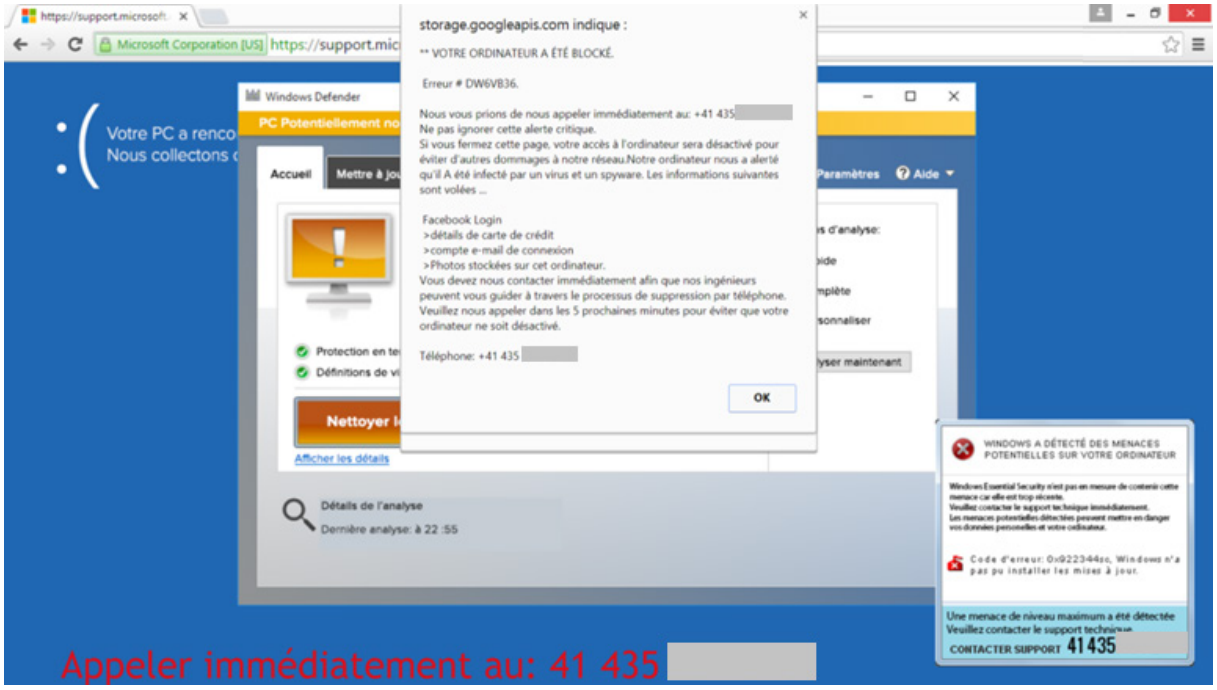

Figure 3: Example of a pop-up on screen. This is not a real navigation bar; it is an image which gives the impression that the user is actually on the Microsoft website.

The basic tips on how to react to this new technique remain the same: Microsoft and other companies will never spontaneously call you to resolve a computer problem. In such cases, it is strongly recommended that you hang up immediately. If scammers do obtain remote access, it is advisable to reinstall the operating system and reset all the passwords used on the computer in question.

Any pop-up warnings that do appear will usually disappear when the browser is closed. If the pop-ups remain on screen, you can close these using the Task Manager. As these types of pop-ups tend to come from dubious websites, avoiding such sites as much as possible will greatly reduce any risk.

Recommendation:

You can find more information on the Microsoft website.

INFO

https://blogs.technet.microsoft.com/mmpc/2017/04/03/tech-support-scams-persist-with-increasingly-crafty-techniques/

https://www.microsoft.com/en-us/safety/online-privacy/avoid-phone-scams.aspx

4.3.5 Phishing with "Data URL" function

On the one hand, attackers are constantly on the lookout for new ways in which to deceive internet users, and on the other they try to make it as difficult as possible for security service

providers to deactivate fraudulent websites. One such method is the misuse of the so-called "data URL" browser function to commit phishing attacks. Although this practice is not new, it was used again in March 2017 for phishing attacks. A "data URL" allows data to be directly embedded in a link, as if it were an external resource. The advantage is that the entire contents of a website can be placed directly in the link, without the usual need to download it from a web server. This means that the internet page is not stored on a web server and so cannot be deactivated by any security service providers.

The webpage which is embedded in a link differs from a normal website as the URL shown does not start with the usual "https://" but rather with "data:text/html" and is very long. However, a fraudster can make a victim believe that the link directs to the web server of an email provider or a credit card company. This is done by cleverly selecting the first rows and thus the area which is visible in the browser's address line. The fraudster designs the launch page of the "data URL" so that only the link of the relevant company is visible (cf. image below). The rest of the very long link, which contains the page's entire source code, disappears into the rows which are not shown.[25]

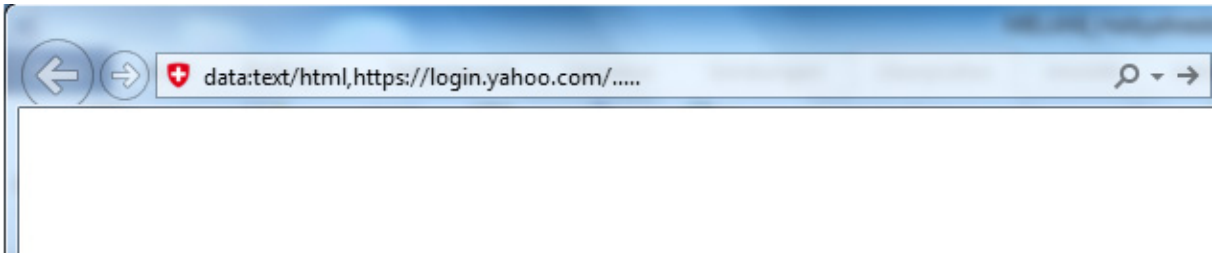

Figure 4: "Data-URL" of an embedded website which supposedly directs to the Yahoo login page. In reality, the site is an embedded website created by fraudsters

4.4 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. Numerous crimeware infections were again recorded in the first half of 2017. As in previous years, the majority was 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 which was both discovered and eliminated in 2008. In second and third place come "spambot" and "cutwail" malware which specialise in the sending of spam and malware. In fourth place is the Mirai botnet, which infects devices in the internet of things and became known after its attack on the internet service provider Dyn. The first e-banking Trojan Dyre follows in ninth place.

[25] https://thehackerblog.com/dataurization-of-urls-for-a-more-effective-phishing-campaign/index.html (as at 31 July 2017).

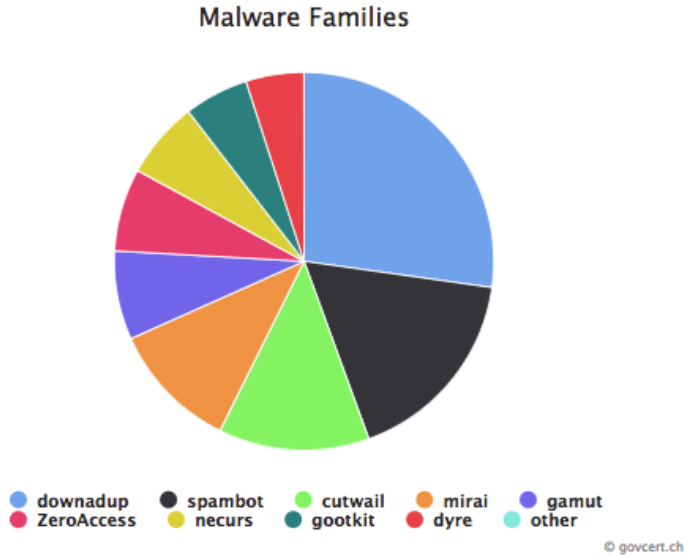

Figure 5: Breakdown of malware in Switzerland known to MELANI. The reference date is 30 June 2017. Current data can be found at: http://www.govcert.admin.ch/statistics/dronemap/

4.4.1 Increased misuse of federal offices and well-known companies for sending malware

Scammers are increasingly sending emails in the name of federal offices in order to make them appear as official as possible and thus give their fraud attempts a better chance of success. For example, emails circulated which were supposedly from the Federal Tax Administration (FTA). The recipients were given the prospect of a tax refund if they completed the attached document which contained malware. In these cases, the senders' email addresses are falsified.

Betreff: Fragen zu der Steuererklarung
Datum: 3. Mai 2017
An: [redacted]

Guten Tag,
mein Name ist [redacted] ich bin Steuerprüfer von Ihrem Bezirk.
Es haben sich einige Fragen zu Ihrer Steuererklärung ergeben.
Dieses Dokument enthält eine Liste von Fragen zu Ihrer Steuererklärung sowie meine Telefonnummer.

Mit freundlichen GRÜSSEN,

[redacted]

Eidgenössische Steuerverwaltung

Diese Nachricht und jegliche Anlagen sind vertraulich und unter Umständen geheim oder anderweitig vor einer Offenlegung geschützt.

Falls Sie nicht der beabsichtigte Empfänger sind, ist es Ihnen nicht gestattet, diese Nachricht oder eine Anlage zu kopieren oder ihren Inhalt gegenüber irgendwelchen anderen Personen offenzulegen.
Falls Sie diese Nachricht versehentlich erhalten haben, setzen Sie den Absender bitte umgehend davon in Kenntnis, und löschen Sie die Nachricht und jegliche Anlagen aus Ihrem System.

Figure 6: Example of a fraudulent email sent in the name of the Federal Tax Administration (FTA)

Attackers also use well-known company names as the sender so that the emails look legitimate. Payment instructions and attempted parcel deliveries from DHL and Swiss Post are popular with attackers. One well-known example from February 2017 involved fake Swisscom bills which attackers used to try to spread Dridex malware.

Attackers also use court summons or emails which appear to be from the cantonal police in order to intimidate recipients and trick them into clicking on a link or attachment.

Conclusion:

Attackers want to catch users off guard. Their aim is to arouse victims' curiosity or intimidate them so that they can be tricked into carrying out a careless action. In the majority of cases, a forgery can be quickly spotted. For example, the Federal Tax Administration only communicates by post and never by email. Fraudulent emails result in a high volume of reports to the companies affected by the fraud which creates extra workload for them.

4.4.2 Malware: care should be taken - regardless of the operating system

MacOS operating system users should also be prepared for malware attacks via Microsoft Office documents: security researchers have discovered Word documents in circulation which contain macros specifically designed for MacOS. If a user opens a manipulated document and allows the macro function to be activated despite the warning notice, the malware it contains will verify whether the Little Snitch safety tool is active. If this is not the case, malicious code is downloaded and a backdoor is installed on the Mac. [26]

Other attacks on MacOS contained a ZIP file attachment which allegedly contained the detailed invoice for a supposed order. The aim was to install the Retefe banking Trojan on these computers. Retefe is a malicious program well-known in Switzerland which attackers, until now, had only used on Windows operating systems.

In order to determine a particular victim's operating system and install the correct version of the malicious software, the criminals first attempt to send an unsuspicious email which automatically provides the attacker with the required information. The email contains a tiny image (1x1 pixel) which is almost invisible to the recipient of the email. When the image is downloaded (which can happen automatically depending on the email configuration), a connection is established with the attacker's server where the image is stored. At the same time, a wide range of information concerning the computer's configuration, including information on the operating system being used, is automatically transferred. This allows the criminals to link the email address with the computer's configuration. In a second stage, they then send an email which is designed for the relevant operating system.

[26] https://www.digitaltrends.com/computing/macos-suffers-first-word-macro-virus/ (as at 31 July 2017).

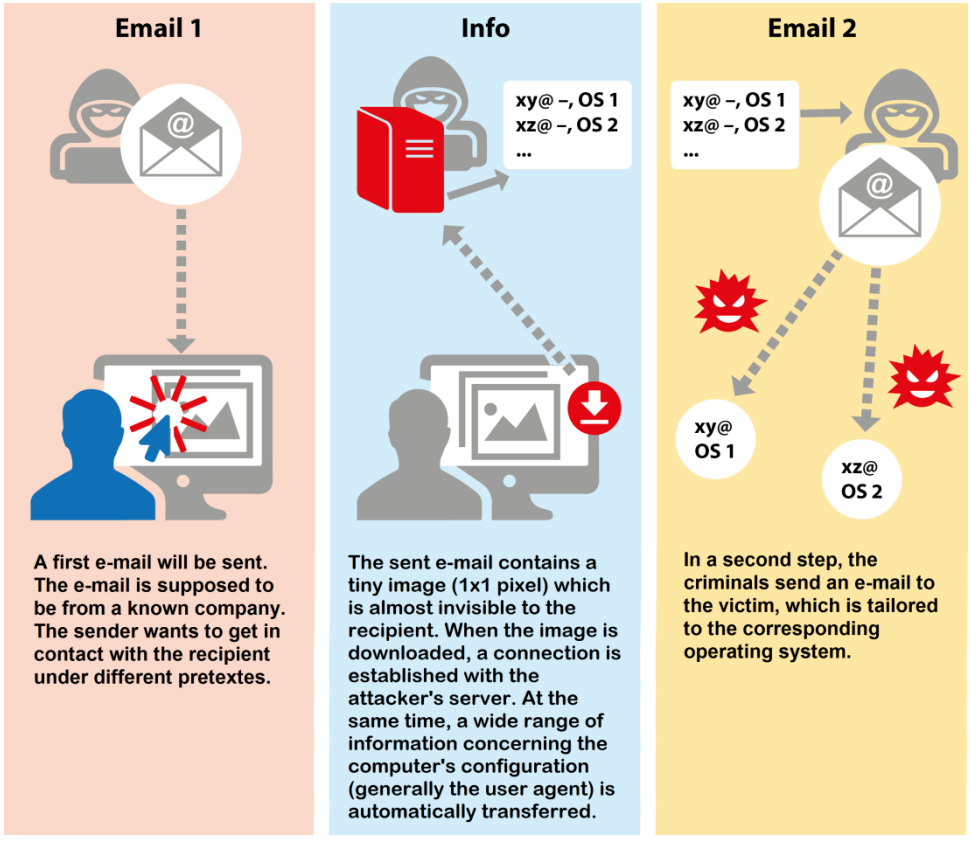

Figure 7 Schematic process: how fraudsters determine which operating system a particular victim has

5 Situation internationally

5.1 Espionage

5.1.1 Managed IT service providers targeted by APT10

Since 2009, the APT10 espionage campaign which probably originated in China and is also known as menuPass, CVNX, StonePanda and POTASSIUM, has targeted a variety of industrial sectors and state institutions. Above all the attackers apparently have their sights set on military installations of various nations and on the US.

In April 2017, the security service provider BAE System, in collaboration with the auditing and consulting firm PwC and the UK National Cyber Security Centre, published the findings of an investigation into recent activities of APT10. According to this investigation, APT10 has carried out two attack campaigns since around the second half of 2016: the first was against Japanese organisations and the second concentrated at a global level on several important managed IT service providers (MSPs).

In the first campaign, the new ChChes Trojan was used. This Trojan uses a certificate from the Hacking Team data leak of July 2015.[27] According to what we know up to now, APT10 is

[27] cf. Semi-annual report 2015/II, section 5.1.1

the only hacker group which uses this specific malware. The two known types of malware PluX and Poison Ivy, among others, were spread with the help of targeted emails. The emails contained files disguised as a Word document containing an icon which after clicking downloaded malware. The emails with bogus sender addresses and topical subject lines such as "The impact of Trump's victory to Japan" were sent to employees of Japanese pharmaceutical companies and the US branch of Japanese firm two days after the US presidential elections.[28]

The MSPs attacked in the second campaign provide support to big organisations in the management of their IT infrastructures. They are an attractive target because they have direct access rights to their clients' systems and data. Probably the MSPs were not the actual target but just served to provide access to the networks of numerous, big companies. This clearly shows that one should therefore carefully select one's partners. This in particular when security is outsourced to an external company.

MSPs were attacked with the PlugX spyware tool which is used by diverse groups. The backdoor virus RedLeaves developed recently is also used.

However, APT10 attacks not just using new tools, the command-and-control infrastructure was also expanded considerably in the period under review. This suggests that this group is very professional and has large sums of money at its disposal. Moreover, the target spectrum has been expanded considerably: it is no longer just the US defence sector or the technology and communications sector which is being attacked but also various other industry sectors throughout the world. Systems in the UK, the USA, India, Japan and other countries were affected.

5.1.2 Siblings spy on 16,000 people

Cyber espionage and theft of sensitive data from high-ranking politicians have become popular ever since the cyber attack on the democrat party leadership in the USA (cf. section 6.2). Italian politicians have also been the victims of a similar attack. But in this case no foreign government was responsible. On 10 January 2017, the Italian brother and sister Giulio and Francesca Maria Occhionero were arrested.

In the case of the malware used, it was a creation of their own of an executable, portable and hidden Win32PE file. Even though it was developed by inexperienced criminals who were not concerned about their own security, it remained undetected for about three years and spied on 16,000 people. The attack was rumbled when the security officer of ENAV S.p.A (Italian national air navigation service provider) contacted the Italian postal police due to a suspicious email which spread the malware. The alleged perpetrators and developers of the malware had left clues behind when registering the IP addresses and when the data was stolen. This was how the police were able to find out the names of those responsible. As the brother and sister in addition conducted their communications via WhatsApp, which was unencrypted at that time, the suspicion was able to be confirmed.

---

https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2015-2.html (as at 31 July 2017).

[28] https://researchcenter.paloaltonetworks.com/2017/02/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/ (as at 31 July 2017).

The campaign was directed at government and business representatives. Famous victims were Italy's former Prime Minister, Matteo Renzi, Mario Draghi, President of the European Central Bank and Vatican dignitaries. Members of a freemason lodge were also attacked. Trendmicro, the IT security company, estimates that the brother and sister were thus able to steal about 87 gigabytes of sensitive data. The brother and sister could have been able to use the data which came from the financial sector for their own benefit as they owned the financial advisory firm Westland Securities. It has yet to be determined whether and to whom the information was to be sold.

5.1.3 Kaspersky top manager arrested in Russia on account of treason

Online activities can be dangerous. However, this quite broadly-based claim is not only applicable to potential victims and criminals. Even researchers in the area of information security sometimes live dangerously when they deal with information on the security of certain countries. Ruslan Stoyanov can confirm this: he was responsible at Kaspersky for computer incidents investigation and was arrested at the end of 2016 and accused of treason. The company which is well known for cyber security distanced itself from this incident and stated that "our employee has been arrested due to incidents which occurred before he was employed at Kaspersky".[29]. The Russian authorities did not comment in any greater detail on the arrest. However, Stoyano is apparently being accused of disclosing secret information to US companies including the IT service provider Verisign which in turn apparently released the information to the US intelligence services. The Deputy Head of the Cyber Division of the Russian Secret Service, Sergei Mikhailov, and another employee, Dmitry Dokuchayev, are also accused of the same crime. The Deputy Head of Verisign denied that the reports which were released to the government authorities and other clients could have contained state secrets. However, he did not comment specifically on the Stoyanov case.

5.1.4 APT32 – espionage carried out by Vietnam?

Sometimes espionage campaigns also originate from regions which are away from the limelight of such incidents. This is the case for example with the OceanLotus Group which was discovered in 2014 by SkyEye Labs. It became well known, however, only recently through enquiries carried out by the security firm FireEye and since then bears the name APT32. The hackers have probably been active since 2013 and their actions seem to serve Vietnam's interests. The targets of the attacks were not just diverse companies with economic interests in Vietnam, the healthcare system, the Vietnamese media and foreign, above all Chinese, governments but also dissidents and activists. FireEye discovered twelve massive attacks.

APT32 works with malware software packages which are attached to commercially available computer programs. On the basis of the targets attacked, it can be assumed that government-run organisations were involved. However, the Vietnamese government stated that it had no knowledge of the activities of OceanLotus.

For the most recent attacks, the APT32 group used Microsoft documents with malicious macros which were sent to victims via email. The attacks were aimed at the Vietnamese subsidiary of a consulting firm operating worldwide, at members of the Vietnamese diaspora in Australia, at employees of the Philippine government and at the Vietnamese subsidiaries of two

[29] http://www.forbes.com/sites/thomasbrewster/2017/01/25/russia-kaspersky-treason-arrest/#1ce5f9174a68 (as at 31 July 2017).

producers of consumers goods in the Philippines and in the USA. The attackers used simple social engineering to convince the victims to activate the macros.

5.1.5 Misuse of commercial espionage software

Pegasus is a sophisticated espionage software, which was specifically developed for mobile phones and is able to infiltrate both iOS and Android systems. It was developed by the Israeli surveillance company NSO and is only sold to governmental institutions to combat terrorism and crime. All activities on a mobile device can be monitored with Pegasus. However, there are now significant grounds to suspect that the NSO spyware, in some cases, has been used for special economic interests and not for the intended purposes.

The Citizen Lab and Lookout Security[30] security companies reported in August 2016 already about Ahmed Mansoor, a well-known human rights activist from the United Arab Emirates. He became a victim of this spyware. In Mexico, the software is said to have been used in two different operations.

Between July and August 2016, Pegasus targeted an important scientist at the Mexican National Institute for Public Health (INSP) and the directors of two Mexican NGOs who are involved in the treatment of obesity. All three target persons supported the so-called Soda Tax, a measure intended to restrict consumption of sweetened beverages and which had been introduced in 2014. As anticipated, the tax led to a reduction in sales of these products which, as expected, sparked off discontent in the food sector. In June 2017, Citizen Lab publicised in an article that attempts were being made to attack journalists, lawyers and activists who were fighting for human rights or were investigating corruption of Mexican government authorities using malware.[31] The large proportion of infection attempts took place in August 2015 and between April and July 2016, as the allegations mentioned above began to accumulate against the President and the government. Both times, the attacks were targeted and had been carried out via text message. The attackers had tried using social engineering techniques to make the recipients click on a link in which an espionage program was hidden. When the target person did not fall for the attempt, family members were then targeted. This explains how the wife of an anti-corruption activist received a text message with a link to alleged photographic evidence that her husband was cheating on her.

5.2 Data leaks

After the record-breaking data leaks during 2016 such as the half a billion customer records at Yahoo[32] or the more than 100 million sets of access data in the business and employment-oriented social networking service LinkedIn[33], at the start of the new year, reports about personal data which had been lost were publicised. In section 6.3 we highlight in addition the

---

30 https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/ (as at 31 July 2017).

31 https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/ (as at 31 July 2017).

32 cf. MELANI Semi-annual report 2016/1, section 5.2.1 https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2016-1.html (as at 31 July 2017).

33 cf. MELANI Semi-annual report 2015/2, section 5.2.2 https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2015-2.html (as at 31 July 2017).

legal changes in Europe within the scope of the EU General Data Protection Regulation (GDPR) which will also involve changes when dealing with these types of incident.

5.2.1 Unwanted transparency in the case of voter profiles of the US Republicans

Companies commissioned by the Republicans in the 2016 US election had to investigate potential voters. Apparently these firms did not take securing the servers where the data was saved too seriously. Researchers from the UpGuard[34] company found the compiled datasets unsecured on a cloud server of the firm Deep Root Analytics. 1.1 terabytes of data which had been compiled by this and two other contractors was publicly accessible in the Amazon cloud. This included personal information such as names, dates of birth, addresses, telephone numbers and voter registration details as well as voter ethnicities and religions of over 198 million American voters “modelled” by the firms. This corresponds to almost all of the USA voter base. Deep Root Analytics when speaking to the paper the Intercept[35] referred to a configuration error in the access rights as the cause of the data leak.

5.2.2 Protected from DDoS but confidential stored content dispersed

The firm Cloudflare made a name for itself with its protection from DDoS attacks. However, as a result of a misconfiguration of server software, partly sensitive memory content was dispersed by third-party websites to the visitors of other clients. Tavis Ormandy, a security researcher in the Google Project Zero noticed that over several months when websites were called up which firstly displayed content delivery network Cloudflare[36], in addition to the requested websites, secret information from other clients was also made public. The error was called Cloudbleed with reference to the SSL bug Heartbleed on social media.

Ormandy is well known for focussing on firms which promise to provide protection against threats on the internet. Cloudflare stated that there were no signs that anybody else apart from the Google researchers had noticed the error. The risk remains that data in caches of search engines and websites which indexed web pages will continue to be accessible to unauthorised persons.

5.2.3 Personal data leak damages confidence in Indian electronic identification (eID)

In order to make flows of money in the country more transparent, India wants to create incentives for more card payments and less cash payments to be made. This will be achieved by using the established online identity project Aadhaar which manages the basis for the unique identity database (UID) which is used for the authentication and authorisation of card payments.

---

[34] https://www.upguard.com/breaches/the-rnc-files?utm_campaign=RNC%20Files&utm_source=upguard_home&utm_medium=breakingnewsbanner, (as at 31 July 2017).

[35] https://theintercept.com/2017/06/19/republican-data-mining-firm-exposed-personal-information-for-virtually-every-american-voter/ (as at 31 July 2017).

[36] A content distribution network is a network of regional distributors and servers connected via the internet through which content, in particular large media files are delivered.

The Indian Centre for Internet and Society (CIS)[37] made public that 135 million card data sets had been leaked which were linked to 100 million bank accounts. It is not the actual Aadhaar database that was responsible for the data leak. The problem was to be found in at least four government projects which complete Aadhaar data with their own data.

The incident clearly illustrates the risks which accompany the use of unique online identities and must as far as possible be restricted. For the users, just slight negligence by one of the partners can cause serious damage to the users' personal privacy and can undermine confidence in this project for a long time.

5.3 Industrial control systems (ICSs)

The focus of this section is on new findings about the malware used which was responsible for a power outage in Ukraine for the second time in December 2016.[38] Additionally, televisions, sirens, surveillance cameras and hotel room doors, which can also be included under the term "industrial control systems", are among the victims in the first half of 2017.

Malware is constantly being discovered even in operators of industrial control systems. A study of the MIMICS (Malware in Modern Industrial Control Systems)[39] project by the cyber security firm Dragos which is active in the ICS environment, comes to the conclusion that operators of industrial control systems have to struggle against the same types of malware as the other companies. A purely eBanking Trojan can indeed do little damage in a control system. By contrast, if the files required for operation are encrypted, ransomware can render the device or the entire system inoperable. This was how for example smart TVs[40] and surveillance cameras[41] in Washington DC were victims of encryption Trojans. Huge damage was done by the Brickerbot[42/43] malware which devastatingly brought vulnerable devices in the internet of things to a standstill. All of these attacks are certainly serious for those concerned but are actually not explicit attacks on the operation of the respective control systems.

---

37 http://cis-india.org/internet-governance/information-security-practices-of-aadhaar-or-lack-thereof-a-documentation-of-public-availability-of-aadhaar-numbers-with-sensitive-personal-financial-information-1 (as at 31 July 2017).

38 cf. MELANI Semi-annual report 2016/2, section 5.3.1. https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2016-2.html (as at 31 July 2017).

39 https://dragos.com/blog/mimics/ (as at 31 July 2017).

40 https://www.heise.de/security/meldung/Erpresser-Botschaft-in-Dauerschleife-Smart-TV-von-LG-mit-Ransomware-infiziert-3584043.html (only available in German) (as at 31 July 2017).

41 www.theregister.co.uk/2017/01/30/ransomware_killed_70_of_washington_dc_cctv_ahead_of_inauguration/ (as at 31 July 2017).

42 https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-102-01A (as at 31 July 2017).

43 http://www.zdnet.com/article/homeland-security-warns-of-brickerbot-malware-that-destroys-unsecured-internet-connected-devices/ (as at 31 July 2017).

5.3.1 Industroyer/CrashOverride – malware communicates independently with substations

After the intensive reporting[44/45] at the start of this year, things quietened down surrounding the alleged cyber attack on the electricity supply in the north of Kiev in December 2016. However, the security researchers involved were working intensively in the meantime on finding out the causes of the power outage. On 12 June, the IT security company ESET and the company Dragos which specialises in IT security in industrial control systems coordinated the publication of the results of the malware samples examined which they had named "Industroyer"[46] and "Crashoverride".[47] Crashoverride is the first known malware framework which was specifically designed to attack electrical grids. After Stuxnet, Havex and Blackenergy 2, it is only the fourth malware which is tailor-made for industrial control systems. In addition to Stuxnet, Crashoverride is only the second malware which can autonomously influence the physical process. As Figure 8 shows, the launcher components are able to execute four different modules to influence industrial protocol communication which are frequently found in the operation of power grids. The framework has a modular design so that with a reasonable effort other protocols can be integrated for future targets. Dragos names the player behind the ELECTRUM malware which according to statements from Dragos analysts has connections to the Sandworm group. These are in turn being blamed by various security service providers[48] for the attacks on the electricity supply in Ukraine in 2015 and 2016.

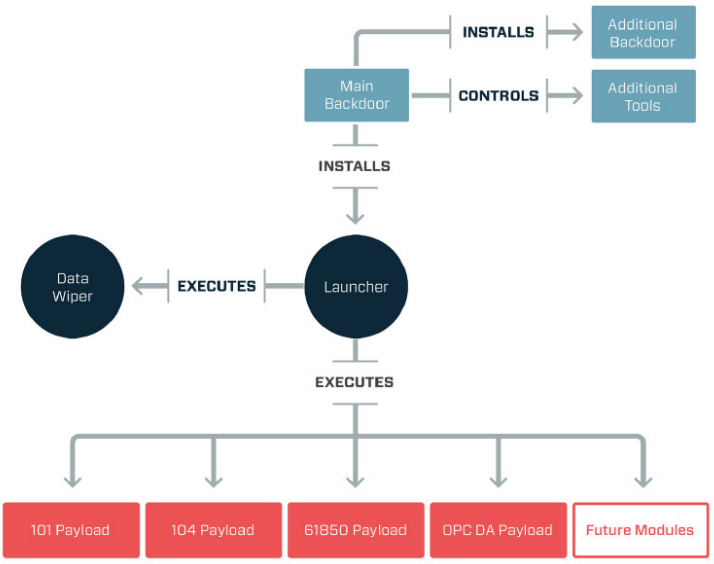

Figure 8: Schematic layout and interaction of the Crashoverride modules (source: *https://dragos.com/blog/crashoverride/*)

44 http://www.bbc.com/news/technology-38573074 (as at 31 July 2017).

45 https://nakedsecurity.sophos.com/2017/01/16/ukraine-power-outages-the-work-of-cyberattackers-warn-experts/ (as at 31 July 2017).

46 https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/ (as at 31 July 2017).

47 https://dragos.com/blog/crashoverride/ (as at 31 July 2017).

48 https://www.wired.com/story/russian-hackers-attack-ukraine/ (as at 31 July 2017).

5.3.2 Radio hackers set off alarm sirens at midnight

Always on the first Wednesday in February, the annual siren test takes place at midday in Switzerland so that alerting the population in the event of a disaster functions properly. That the sirens went off shortly before midnight for 95 minutes on 7 April 2017 in Dallas to warn of non-existent tornados was on no account due to a test being carried out. Initially it was assumed that it was an attack on the emergency services systems in this Texan city. However, the authorities were quickly able to provide the information that nobody had gained access to these networks. The reason for the false alarm was that the sirens had been controlled by radio signals which are transmitted by the national weather service in the event of an incident. In the case of older sirens, however, these radio signals are not secured or even encrypted, they are openly transmitted. Devices which can transmit radio waves of this nature, so-called software defined radios (SDRs), are becoming more and more affordable. Practically anybody can use these devices which is why it was only a matter of time before these systems were misused. The attacker just had to try out all possible commands on the corresponding frequency. The success of this method can be confirmed by those present in Dallas whose ears bore the brunt of the onslaught.

5.3.3 The encrypted lock

Many hotels no longer have traditional keys, instead they provide their guests with a card on which the code to open the respective hotel room is stored. The advantage is obvious. In addition to being more convenient for the guests, in the event of the key to the room being lost, the old code can simply be revoked and a new code will be assigned to the door. This progress also has drawbacks as the Romantik Seehotel Jägerwirt in Austria discovered. On its opening weekend, the fully-booked hotel was suddenly unable to open any of the hotel room doors. The reason for this was an infection caused by ransomware.[49] In addition to the booking and payment systems, the server of the key cards was also encrypted. Consequently neither the hotel room doors could be unlocked nor could the key cards be reprogrammed. In desperation, the hotel paid the ransom in bitcoins of almost EUR 1,500. The extortionists subsequently decrypted the infected devices, however, they tried to keep a backdoor in the systems open. The hotel then replaced some of the devices and got additional protection for the network to prevent further infection. After the unpleasant experience with the digital locking system, when the next renovation takes place the Jägerwirt is once going to convert back to conventional keys.

[49] https://www.thelocal.at/20170128/hotel-ransomed-by-hackers-as-guests-locked-in-rooms/ (as at 31 July 2017).

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 (DDoS, defacements, drive-bys)

5.4.1 Networks of financial institutions redirected for seven minutes

At the end of April 2017 the network traffic of several financial service providers, including that of the Visa and Mastercard credit card companies, was redirected for almost seven minutes to a Russian telecommunications provider. Anomalies in the so-called Border Gateway Protocol (BGP) occur regrettably time and again. BGP regulates the traffic between the different subnetworks of the internet and thus determines which data packet will be forwarded via which provider. However, what is striking about this case is that the faulty command of the Russian telecommunications provider Rostelecom only concentrated on address blocks of financial services providers and IT security companies. There was a chance that during the time of the misdirection, network traffic was analysed and at worst was even changed. What the misconfiguration caused is so far not known. In particular, it has not been possible to clarify whether this misconfiguration was caused by a technical or human error or was even due to a hacker attack.[50]

In another case where the majority of the network of a Brazilian bank was concerned, network traffic was taken over completely for five hours. The attackers succeeded in compromising the DNS service of the bank and was thus able to act as the operator of the bank infrastructure in relation to the majority of the network users. In this way, it would have been possible to spy on transactions, access data was tapped and clients were infected with malware.[51]

5.4.2 Targeted infection via website of the Polish financial regulator

At the start of February 2017, it emerged that malware had been found on various computers of several Polish banks. The infection vector was the website of the Polish Financial Supervi-

[50] https://arstechnica.com/information-technology/2017/04/russian-controlled-telecom-hijacks-financial-services-internet-traffic/ (as at 31 July 2017).

[51] https://www.wired.com/2017/04/hackers-hijacked-banks-entire-online-operation/ (as at 31 July 2017).

sion Authority (KNF) which was compromised by attackers with a so-called drive-by infection. In addition, one of the local JavaScript files was changed in such a way that a further, external JavaScript file was downloaded which in turn downloaded malware.[52] Simply by surfing on this website, it was possible for the visitor's computer to become infected with malware. Because the majority of people accessing the Financial Supervision Authority are from the financial environment, the attacker had probably planned a very targeted attack. The malware then tried to connect with foreign servers. According to the BadCyber portal, the attackers managed in some cases to get control of computers in bank infrastructures.[53]

It turned out that the targeted attack on the Polish financial institutions was only part of the attack. A website infection of the same type was found on the website of the Mexican banks and stock exchange supervisory authority. The exploit kit was configured in such a way that only visitors were infected who surfed to the website with one of over 150 predefined IP addresses. These 150 IP addresses were able to be allocated to 104 different organisations in 31 countries. Many of these companies were banks, a smaller proportion were telecom and internet companies. According to current information, no Swiss organisations were affected. The attacks were able to be traced back to October 2016 at least.

The previously unknown malware Ratankba[54], downloaded a hacking tool which has links to Lazarus, after it had made contact with the control server. The Lazarus group is being connected with attacks on US and South Korean targets which have been taking place since 2009. Lazarus is also being associated with the attack on the Bangladesh national bank in 2016.[55] Further analysis by Kaspersky shows that the Lazarus group contains a subgroup which is specially geared to attacks on the financial system. The group emerged in the past also under the name BlueNoroff. The perseverance and persistence of this player will not spare the international financial market in the future either.

5.4.3 Botnet spreads rumours about market manipulation

Necurs is a traditional botnet for sending spam messages and is well known for the wide distribution of the Locky ransomware or the eBanking Trojan Dridex. According to MELANI statistics, Necurs is in seventh place on the list of the most widespread malware in Switzerland.[56] In the period under review, it was noted how scammers used the dissemination of spam to manipulate penny stock share prices[57]. In a spam wave sent by Necurs, an announcement was made about an alleged takeover in the drone market. The recipients who could not resist the temptation of a fast buck subsequently bought shares in the company advertised and thereby drove up the share price. The attackers had already bought shares in

---

52 https://badcyber.com/several-polish-banks-hacked-information-stolen-by-unknown-attackers/ (as at 31 July 2017).

53 https://www.theregister.co.uk/2017/02/06/polish_banks_hit_by_malware_sent_through_hacked_financial_regulator/ (as at 31 July 2017).

54 https://www.symantec.com/connect/blogs/attackers-target-dozens-global-banks-new-malware-0 (as at 31 July 2017).

55 cf. Semi-annual report 2016/1, section 5.4.1 https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2016-1.html

56 cf. current MELANI semi-annual report 2017/1, section 4

57 http://blog.talosintelligence.com/2017/03/necurs-diversifies.html (as at 31 July 2017)

the company before the spam was sent and sold these shares after the self-induced rise in the share price with a sizeable profit. The example of this pump-and-dump attack shows how internet criminals time and again search for new ways to use their infrastructure and skills for lucrative ends, but are also ready to use tried and tested methods.

5.4.4 Patient database in the hands of extortionists

After the damage caused by WannaCry in hospitals in the UK, an incident in a plastic surgery clinic in Lithuania also shows how sensitive patient data is and how important it is to correspondingly protect it. The attackers who called themselves Tsar Team, blackmailed the clients of this clinic in over 60 countries with the publication of patient photos which had been copied from the clinic's database. As proof, 25,000 of these photos were published on the internet.[58] Before the extortionists contacted the clients with demands for amounts between EUR 50 and EUR 2,000, they tried to sell the entire database for half a million pounds sterling in bitcoins to the clinic. The clinic did not meet the extortionist's demands. How many clients paid the ransom amount to the extortionists is not known. The name Tsar Team also crops up in connection with Sofacy. However, up to now it has not been possible to confirm a connection. It is also conceivable that the attackers just used the well-known names of the espionage group to be able to exert more persuasive pressure on the victims.

5.4.5 SS7 – Old standard in eBanking authentication

To log in securely to an internet service such as eBanking, a further authentication method is generally used alongside the password. Ideally, this second authentication is performed via a second, independent communication channel. Here many providers opt for text messages via mobile phones. Because most mobile phones today are small computers, they can be infected with malware which, among other things can intercept messages and forward them to the scammers. Moreover, many banking transactions are now often conducted using a smartphone, with the result that login and the second authentication are performed on the same device. The additional security which the text message authentication should provide is missing. MELANI has already dealt with the problem areas which arise when using text messages as the second factor in authentication in the last semi-annual report.[59]

At the start of March 2017, yet another opportunity was actively used by criminals to intercept text messages sent by the bank for the purpose of authentication. As the German mobile communication provider O_2 confirmed to the Süddeutsche Zeitung, a vulnerability in the SS7 protocol which has been known about for several years was used to allow improper transactions in German bank accounts to be carried out.[60] To this end, the criminal misused a function in the SS7 protocols which is actually there to permit international roaming. Mobile phones can register with a foreign network abroad; the corresponding foreign network operator notifies the home network of the subscriber and text messages are subsequently forwarded to 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

---

58 https://www.theguardian.com/technology/2017/may/31/hackers-publish-private-photos-cosmetic-surgery-clinic-bitcoin-ransom-payments?CMP=twt_gu (as at 31 July 2017).

59 cf. MELANI semi-annual report 2016/2, section 6.2 https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/halbjahresbericht-2016-2.html (as at 31 July 2017).

60 https://www.theregister.co.uk/2017/05/03/hackers_fire_up_ss7_flaw/ (as at 31 July 2017).

be intercepted there. That 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 permit fraudulent activities, or work together with scammers.

Conclusion:

In several countries the initial hurdle for dubious network participants has been lowered significantly. At the same time, not all mobile operators conduct plausibility tests. This problem has been addressed time and again since 2014. To circumvent authentication by text message at the network level, this, however, requires more special expertise. However, well-organised criminal groupings and state players already have the required skills. For fraud in eBanking, the simultaneous infection of the computer and smartphone of a user probably remains the more established and more lucrative method. Because of this alone, providers of online services will, in the medium-term, change to alternative methods of authentication.

5.5 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.

5.5.1 Deutsche Telekom disruption due to Mirai: arrest

In the last semi-annual report, the Mirai botnet was covered extensively.[61] Mirai is a malware targeting the Linux operating system, which is used in many devices in the internet of things. On 27 November 2016, an attack with this malware led to an internet outage affecting 900,000 Deutsche Telekom customers. The reason for the outage was the deployment of a new version of the malware Mirai which, due to faulty programming, caused a crash instead of an infection of home network routers of Deutsche Telekom.

A Liberian hacker who was behind this attack has been arrested in London in the meantime. His explanations demonstrate impressively how multi-dimensional and complex the background to such an act can be. The arrested person explained that he was approached by a Liberian telecommunications company to sabotage competitor businesses. To carry out a DDoS attack, he then adapted the freely available malicious code of the Mirai botnet and supplemented it with a new attack method which can exploit the remote maintenance function of certain routers. It was precisely this newly implemented function which then apparently caused the crash of the router at Deutsche Telekom. The accused also advertised his botnet on the internet for rental. In court, however, he said that this had only been a smoke screen for his actual client. He himself had hoped to get a job with his client. In fact the Libe-

[61] cf. MELANI semi-annual report 2016/2, section 3 https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/halbjahresbericht-2016-2.html (as at 31 July 2017).

rian provider Lonestar Cell was attacked in January 2017 which led to a partial outage in mobile phone reception and to an overload in the undersea cables to Africa.

The German court only took account of the attack on Deutsche Telekom and thus imposed a suspended sentence of only one year and eight months on the attacker. However, he was not released and ended up in extradition custody. The UK authorities are accusing him of a number things. In addition to the attack already mentioned on Lonestar Cell, he is also said to have extorted five-figure amounts from UK big banks.

5.5.2 Bootlegger of Apple internal client data arrested

The Chinese police arrested more than twenty employees of Apple partners who stand accused of stealing client data from the iPhone manufacturer and then selling this data on the black market.[62] The employees who were mainly employed in sales and marketing accessed databases with information about iPhone and iPad users. Among other things, the data contained names, mobile phone numbers and Apple IDs. The perpetrators offered this data for prices between USD 1.50 and USD 26.50 per data set to interested buyers in the digital underworld. Up until the arrests were carried out, more than USD 7 million was gathered from sales. Insider attacks of this nature show clearly that not just preventive protection measures against attackers from outside the organisation have to be implemented but also internal processes and systems to recognise ongoing attacks in order to protect one's own data.

A good start to not become a victim of attacks of this nature is the MELANI factsheet on ICT security in SMEs:

Checklist on IT security for SMEs

https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/checkliste-online-auftritt-kmu.html (not available in English)

SME portal of the federal government

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

[62] https://www.tripwire.com/state-of-security/latest-security-news/apple-employees-detained-selling-user-data-chinese-black-market/ (as at 31 July 2017).

6 Trends and outlook

6.1 The role of insurers in cyberspace

If you take the time to read the Ordinance on the Technical Requirements for Road Vehicles (RVTRO), you will discover that doors must be secured against "unwanted opening" but that a locking device is not an explicit requirement for a road vehicle. In principle, vehicle alarm systems are also not mandatory, but if they are used, the RVTRO describes which requirements they have to meet in relative detail.

Even if a car without a door lock did pass as a road vehicle, it is rather unlikely that anyone would consider removing the lock which was installed as standard from their newly purchased car. Firstly, because very few owners are interested in making thieves' work easier and, secondly, because the insurance company would no longer pay out in the event of theft.

There are many other examples of where insurers impose de facto safety standards with their requirements and premium calculations. Some insurance companies do not calculate premiums for works of art based on the value of the painting alone. They also take into account other factors, such as the security measures put in place to protect the item. If these measures meet the current best practice requirements for the domain, the client pays a lower premium.

Cyberspace is highly dynamic and what was considered to be state-of-the-art yesterday is already old hat today. This makes formulating minimum safety standards a continuous and dynamic task. With a view to the wide use of information and communication technologies, safety standards in cyberspace also have to be flexible and adapted to their actual intended purpose. But the specification of governmental regulations is often a slow process.

On the other hand, insurance companies are relatively free to adapt to changes and developments within the framework of their industry. They can impose safety standards on their customers in line with the relevant best practice criteria. This means that insurers often cover measures which are not typically subject to any regulations. The growing cyber insurance market not only offers a business opportunity but also a general chance to increase security culture and, in turn, basic security in cyberspace sustainably.

However, it is not an option to rely on the insurance industry alone to resolve the problem of safety standards in cyberspace over the short or long term. For one, the specialist authorities can respond in a supportive manner by, for instance, making principal-based stipulations within their scope of competency. These would then serve as guiding principles for the insurance industry. With an eye to actual risk calculations, state institutions can also assist in cyberspace affairs with their knowledge of threats and development. Finally, there is the hypothetical possibility an "earthquake of the century" occurring in cyberspace. This would result in theoretically exorbitant losses which would wipe out every insurance company and thus makes it simply impossible to insure certain cyber risks. Finding a solution to this problem, e.g. in line with the state guarantee for earthquake damage above a certain amount of loss, is a challenge for the state and the insurance industry. If they manage to do this, insurers would benefit from planning certainty and thus the possibility to take a more pro-active approach to cyber policies. In the end, it is not only the insurance branch which would win. Businesses, society and the state would also benefit from insurers taking on risks and adopting the relevant risk-minimising requirements.

6.2 Politicians - a popular target for cyber manipulators

The cyber attack on the Democratic National Committee (DNC) in the US which the security firm Crowdstrike attributed to the espionage campaigns Cozy Bear and Fancy Bear[63], was the first in a long line of cyber attacks in which political representatives were the focus. The attacks have shown that the publication of private messages does indeed influence public opinion. According to a blog on The Intercept[64], the hypothesis that cyber criminals actually intended to manipulate the results from the US presidential election is gaining ground. The intention to favour one candidate by harming the competition can also be seen in the so-called "fake news" phenomenon, which increasingly appears during election campaigns.

Technical security measures for government and business networks alone are not enough to protect the state, society and democratic institutions. An increasing number of prominent figures, politically active individuals and elected representatives in particular have seen their private online accounts become the targets of attacks. The purpose of these attacks can be to obtain compromising material or to use an account to make reputation-damaging or manipulative statements.

Following the examples of countries such as Germany and the United Kingdom, MELANI has created a info card list of security measures. The list is intended to help members of parliament protect themselves. The recommendations are, of course, also valid for non-politicians.

6.2.1 Attacks on election campaigns

The cyber attacks during the US presidential elections did not just target the email accounts of Democratic National Committee representatives. According to The Intercept website, a company was also attacked which produces machines for checking ballot cards.[65]

Targeted emails were also sent to over 100 civil servants who were responsible for monitoring the election results. The emails, which contained malware, were well thought out: they were sent to unsuspecting employees at local government organisations. The emails supposedly came from an employee at a company which offers services in the area of e-voting and election software. In order to do this, the company's account had previously been compromised. Between 31 October and 1 November 2016, an email was sent to 122 recipients with a malicious Word document attached which contained a Trojan. The NSA remained guarded over the results of these attacks and any eventual success the malicious emails may have had, as well as any extracted or even manipulated data.

The question is therefore how secure electronic electoral programs actually are. Countries which use such programs should know that they are dealing with critical infrastructures. They should consider which processes will best protect them. If the risk is considered to be too

---

63 cf. MELANI Semi-annual report 2/2016 https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/halbjahresbericht-2016-2.html6-2.html (as at 31 July 2017).

64 https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/ (as at 31 July 2017).

65 https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/ (as at 31 July 2017).

high, extreme solutions must also be taken into consideration. For instance, as is the case in Germany and the United Kingdom, dispensing with such programs.

6.2.2 Honeypot accounts: strategies against infiltration attacks

In December 2016 during the French election campaign, employees' of En Marche! became the target of a spear phishing campaign. Furthermore, the NSA uncovered an infiltration attempt on the French infrastructure and informed the relevant authorities on 5 May 2017. It was no surprise that the attacks intensified towards the end of the campaign. The events surrounding the US presidential election, and the knowledge that they could not offer comprehensive protection, prompted the En Marche! technical team to take preventive action. They opted for a cyber-blurring strategy; creating false email accounts which were to act as honeypots for the attackers. Each false account was filled with ad hoc documents in order to perturb hackers. If the attackers wanted to extract data, they would first have to verify whether the documents were real or not. However, the attackers did not take on this work themselves. They published all 9 gigabytes of files, which included the ad hoc documents. The data was initially published on the US website Pastebin and then shared between 3Chan and WikiLeaks. Despite an attempt to discredit presidential candidate Macron with reports that he was supposed, for instance, to have a secret bank account on the Bahamas, the strategy proved successful. The fact that the data published was in part fake and not particularly revealing, meant that Macron's campaign was not overtly affected.

The quality of the emails used for the attacks was generally considered to be good. Just before the end of the campaign, emails appeared which had supposedly come from Emmanuel Macron's "Digital Director". The emails prompted the recipients to download the attached file in order to protect themselves from cyber attacks. However, the attack proved to be somewhat unprofessional and, furthermore, the attackers left traces. For instance, Russian usernames were found in the documents which had been created or modified. In other cases, the documents had been edited with a version of Microsoft that is only available in Russia. Indications also appeared in the C&C infrastructure that the hacking campaign Sofacy, was behind the attack[66]. The same group was also held responsible for the attacks on the Clinton campaign.

6.2.3 Germany and United Kingdom also targeted

The German Federal Office of Information Security (BSI) reported that, at the end of June 2017, the private email accounts of representatives from business communities and public administration employees were almost flooded with waves of phishing emails.[67] The attempted attacks focused on Yahoo and Gmail accounts. Examination of the attackers' infrastructure showed similarities to the campaigns against the Democratic National Committee in the US and France as described in sections 6.2.1 and 6.2.2.

---

66 https://www.nytimes.com/2017/04/24/world/europe/macron-russian-hacking.html?mcubz=0 (as at 31 July 2017).

67 http://www.zdnet.de/88302365/bsi-warnt-vor-phishing-angriffen-auf-funktionstraeger/?inf_by=59a97d93681db8d9688b45bf (as at 31 July 2017).

On Friday 23 June 2017, the British parliament also became the victim of a cyber attack. It would appear that the email accounts of around 90 members of parliament were hacked. It transpired that the passwords in use were too weak and did not meet the requirements. Once the cyber criminals had hacked the email accounts, they locked the remote access so that the lawful account holders were prevented from setting up more secure passwords.

Recommendation:

Each administration or company can only protect its own network and infrastructure. Mobile devices, email addresses and other IT infrastructure which employees use privately are outside their sphere of influence. Attacks on private networks therefore have more chance of success and it cannot be excluded that government networks will be infected as a direct result. For this reason, the German Federal Office of Information Security has published a set of prevention guidelines. They are aimed at public administration staff and top employees at financial companies but can also be helpful to private individuals. MELANI particularly recommends the following measures which are based on the German Federal Office of Information Security guidelines.

- do not send work emails using private accounts;
- encrypt emails classified as confidential;
- set up two-factor authentication;
- if there is the slightest suspicion that your email account may have been hacked, you should change your password immediately.

MELANI has created an infocard with a list of security measures for members of parliament.

The infocard for members of parliament can be downloaded from the MELANI website

https://www.melani.admin.ch/melani/en/home/dokumentation/Infokarten.html

6.3 New EU General Data Protection Regulation and its impact on Switzerland

The European Union General Data Protection Regulation (EU GDPR) is a regulation that harmonises the standards for processing personal data for private companies and official bodies throughout the EU. The regulation replaces Directive 95/46/EC from 1995. It came into force on 24 May 2016 and is to be applied by all member states after a two-year transitional period, i.e. as of 25 May 2018.

Convinced that a basis of trust is essential in order to found Europe's digital future, the EU is pursuing three goals with its General Data Protection Regulation: the harmonisation of data protection law across Europe, the strengthening of the Single Market by guaranteeing the same economic conditions in the Union and the modernisation of data protection in line with technical developments while maintaining fundamental rights.

The main changes arising from the new regulations can be summarised as: the right to be forgotten; data processing is only permitted with the express content of the person con-

cerned; the right to data portability (to another service provider); the right to be informed if one's own data protection is breached and, finally, a tougher crackdown on regulation infringements. The latter means that for businesses, monetary fines can be imposed of up to 4% of their annual worldwide turnover from the preceding business year.

In contrast to Directive 95/46/EC, which had to be transposed by the member states into national law, the General Data Protection Regulation will apply in all member states from May 2018. In principle, this means that the member states are not allowed to use national regulations to weaken or strengthen the data protection set out in the Regulation. However, the Regulation does contain 70 opening clauses which allow member states to regulate certain aspects of data protection at national level.

The numerous exceptions and resultant legal uncertainty have resulted in criticism of the General Data Protection Regulation from various groups. The Regulation is said to neglect the original objective of the harmonisation, to be too abstract and to make too many exceptions. It is also argued that it will inevitably lead to interpretation difficulties and inconsistencies with national laws which will remain valid. Germany notably warned of a dumbing down of its data protection law. The standards are said to be so technology-neutral that they do not sufficiently deal with the risks information technology faces.

The General Data Protection Regulation is not only applied within the EU but also in third countries such as Switzerland. This means the EU General Data Protection Regulation also applies to all Swiss companies, with or without headquarters in the EU, which offer products and services to persons in the EU (which is most likely the case if their website or webshop does this), process personal data deriving from EU-citizens or if they analyse the behaviour of persons in the EU.

Recommendation:

MELANI recommends adjusting relevant information processing operations, data storage and information assurance to meet the new statutory requirements in good time. Not only can it be assumed that companies will be preoccupied with the implementation of the Regulation and the provision for large monetary fines in the case of data protection violation; it is also expected to inspire criminals to invent new extortion methods.

The total revision of the Swiss Data Protection Act is currently still underway. It can be assumed that the revision will embrace various new elements of the EU General Data Protection Regulation.

7 Politics, research, policy

7.1 Switzerland: parliamentary procedural requests

Item	Number	Title	Submitted by	Submission date	Council	Office	Deliberation status & link
Mo	17.3508	Creation of a cyber security competence centre at federal level	Joachim Eder	15.06.2017	CS	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173508
Mo	17.3507	A cyber defence command with cyber troops for the Swiss Army	Josef Dittli	15.06.2017	CS	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173507

Mo	17.3497	Central contact and coordination unit to combat organised and international computer crime	Marcel Dobler	15.06.2017	NC	FDJP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173497
Mo	17.3496	Obligatory baseline protection for critical power infrastructures	Edith Graf-Litscher	15.06.2017	NC	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173496
Mo	17.3475	Obligation to report serious security incidents in critical infrastructures	Edith Graf-Litscher	15.06.2017	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173475
Po	17.3433	Cyber security in health care	Bea Heim	13.06.2017	NC	FDHA	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173433
Mo	17.3199	Expansion of cyber defence competences	Franz Grüter	16.03.2017	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173199
Ip	17.3136	Cyber security in health care	Bea Heim	15.03.2017	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173136
Ip	17.3103	Challenges in the cyber domain. How should Switzerland pro-ceed?	Joachim Eder	13.03.2017	CS	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173103
Mo	17.3591	Net neutrality. Maintaining the original vitality of the internet	Claude Béglé	16.06.2017	NC	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173591
Ip	17.3452	How can we support the media during the transition to the digital world?	Adèle Thorens Goumaz	14.06.2017	NC	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173452
Ip	17.3277	Are today's legal sanctions enough to control the internet giants?	Jean Christophe Schwaab	02.05.2017	NC	FDJP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173277
Ip	17.3276	Internet advertising that is illegal, hateful or generates funds to finance criminal activities: who is responsible and to what extent?	Jean Christophe Schwaab	02.05.2017	NC	FDJP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173276
Ip	17.3254	Taking advantage of the benefits of modern technology for per-sons with disabilities. e.g. HbbTV	Pascale Bruderer Wyss	17.03.2017	NC	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173254
Ip	17,313	Internet commerce with live animals and animal protection	Daniel Brélaz	15.03.2017	NC	FDHA	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173130
Fr	17.5206	Cyber security. Security stand-ards to prevent hacked devices which are connected to the internet of things being used as botnets	Balthasar Glättli	08.03.2017	NC	EA-ER	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20175206
Ip	17.3069	Do current statistics capture the potential of digitisation?	Ruedi Noser	07.03.2017	CS	FDHA	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173069

Ip	17.3075	Digital gender gap. Which challenges and opportunities does digitisation provide in the working world from a gender perspective?	Sibel Arslan	08.03.2017	NC	EA-ER	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173075
Mo	17.3592	Let the governance of digitisation develop towards a governance model inspired by digitisation	Claude Béglé	16.06.2017	NC	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173592
Ip	17.3533	Increase IT training in Switzerland	Franz Grüter	15.06.2017	NC	EA-ER	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173533
Ip	17.3341	Is the Federal Office of Information Technology a federal office for in and outsourcing?	Stefan Müller-Altermatt	04.05.2017	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173341
Fr	17,104 0	Expansion of mobile networks to support digitalisation in Switzerland	Christian Wasserfallen Radical Free Democratic Group FDP	06.06.2017	NC	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20171040
Mo	17.3498	Mobile telephones: Give Switzerland its competitiveness back!	Yannick Buttet	16.06.2017	NC	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173498
Fr	17.5303	Are drones endangering the safety of national airports?	Priska Seiler Graf	07.06.2017	NC	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20175303
Fr	17.5221	Mountain farmers cut off from the telephone network	Erich von Siebenthal	30.05.2017	NC	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20175221

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 Notes About The «NotPetya» Ransomware

28.06.2017 - A new ransomware, currently named «NotPetya», has begun spreading yesterday. There are many victims, especially in Ukraine, but also large companies have been hit hard such as «Maersk» or «Merck». There are infections in Switzerland as well. As many others we have analyzed the malware and tried to harden evidence about its functioning. As there are many good papers already published, we do not want to repeat all these things but to highlight a few important facts that now can be considered being hardened evidence.

➔ https://www.govcert.admin.ch/blog/32/notes-about-the-notpetya-ransomware

8.1.2 «WannaCry»? It is not worth it!

15.05.2017 - On Friday, May 12th 2017, a ransomware called «WannaCry» hit the cyber space. Among the victims are hospitals in UK, the national telecom provider in Spain and U.S delivery service «FedEx». But WannaCry did not only hit the internet, the ransomware was also very present in newspapers worldwide. It also kept us and our partners from abroad very busy during the last weekend, analyzing the malware, reevaluating the current situation in Switzerland and world-wide, communicating with National Critical Infrastructure, and talking to the press. While we analyzed the threat as well, there are already many good papers on «WannaCry». For this reason we do for once not focus on the exact technical implementation, but try to give a comprehensive overview of this threat and the impact «WannaCry» has, with a focus on the situation in Switzerland.

➔ https://www.govcert.admin.ch/blog/31/wannacry-it-is-not-worth-it

8.1.3 When «Gozi» Lost its Head

04.04.2017 - After our automated unpacking procedure recently failed on a «Gozi» binary (MD5 c1a73ff8fb2836fe47bc095b622c6c50), we were forced to perform a manual analysis - and indeed we found some interesting new features in the first layer of the packer…

➔ https://www.govcert.admin.ch/blog/30/when-gozi-lost-its-head

8.1.4 Taking a Look at «Nymaim»

03.03.2017 - «Nymaim» is active worldwide since at least 2013 and is also responsible for many infections in Switzerland. Sinkhole Data shows that «Nymaim» is responsible for about 2% of infected devices in Switzerland that hit sinkholes the last few days. When we looked at the «Nymaim» trojan in January, we were stunned by their powerful code obfuscation techniques and wrote an «IDAPython» script to deobfuscate the code using the debugger engine. Later we found similar tools already available in the public to do this using code emulation. Nevertheless, we decided to publish a paper about our approach, as it is a very nice case study to demonstrate how debugger orchestration works in «IDAPython», and to explain different disassembly strategies that can be used. Instrumenting the debugger means to set breakpoints in scripts and to run the code in pieces, which has a very dynamic and fascinating impact on the IDA GUI.

➔ https://www.govcert.admin.ch/blog/29/taking-a-look-at-nymaim

8.1.5 The Rise of «Dridex» and the Role of ESPs

20.02.2017 - Last week, we have warned Swiss citizens about a new malspam run targeting exclusively Swiss internet users. The attack aimed to infect them with «Dridex». «Dridex» is a sophisticated eBanking Trojan that emerged from the code base of «Bugat» / «Cridex» in 2014. Despite takedown attempts by the security industry and several arrests conducted by the FBI in 2015, the botnet is still very active. In 2016, MELANI / GovCERT.ch became aware of a handful of highly sophisticated attacks against small and medium businesses (SMB) in Switzerland aiming to steal large amounts of money by targeting offline payment software. During our incident response in 2016, we could identify «Dridex» to be the initial infection vector, which had arrived in the victim's mailbox by malicious Office Word documents, and uncovered the installation of a sophisticated malware called «Carbanak», used

by the attacker for lateral movement and conducting the actual fraud. Between 2013 and 2015, the «Carbanak» malware was used to steal approximately 1 billion USD from banks worldwide.

➔ https://www.govcert.admin.ch/blog/28/the-rise-of-dridex-and-the-role-of-esps

8.1.6 «Sage 2.0» comes with IP Generation Algorithm (IPGA)

30.01.2017 - On Jan 20, 2017, we came across a malware that appeared to be a new Ransomware family called «Sage 2.0». Within a couple of days we were able to collect more than 200 malware binaries across our sensors associated with this new Ransomware. Last week, Brad Duncan also wrote a SANS InfoSec Diary entry on «Sage 2.0», noticing some strange UDP packets sent to over 7'000 different Ips.

➔ https://www.govcert.admin.ch/blog/27/sage-2.0-comes-with-ip-generation-algorithm-ipga

8.2 MELANI newsletter

8.2.1 Schadsoftware: Vorsicht ist geboten - unabhängig vom Betriebssystem

15.06.2017 - Bei der Verbreitung von Schadsoftware via E-Mail versuchen Kriminelle vermehrt, ihre Opfer gezielt anzugreifen. Dabei sind nicht mehr nur ausschliesslich Windows Benutzer im Visier. In den vergangenen Wochen hat die Melde- und Analysestelle Informationssicherung MELANI verschiedene Schadsoftware-Wellen beobachtet, welche sich gezielt gegen Schweizer Nutzende des Betriebssystems MacOS, das von Apple entwickelte Betriebssystem, richteten. Es ist deshalb wichtig in Erinnerung zu rufen, dass unabhängig vom verwendeten Betriebssystem und für alle Nutzenden Vorsicht geboten ist.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/malware---si-raccomanda-prudenza-indipendentemente-dal-sistema-o.html

8.2.2 Zunehmender Missbrauch der Namen von Bundesstellen und Firmen

04.05.2017 - In den letzten Monaten hat der Missbrauch der Namen von Bundestellen und bekannten Firmen als Absenderadresse zugenommen. MELANI gibt Tipps, wie man sich verhalten soll.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/zunehmender-missbrauch-der-namen-von-bundesstellen-und-firmen.html

8.2.3 For secure dealings with the internet of things

20.04.2017 - The 24th semi-annual report of the Reporting and Analysis Centre for Information Assurance (MELANI), published on 20 April, addresses the most important cyber incidents of the second half of 2016 both in Switzerland and abroad. The focal point of the report is the internet of things, which is becoming increasingly significant.

➔ https://www.melani.admin.ch/melani/en/home/dokumentation/newsletter/semi-annual_report-2016-2.html

8.2.4 Social Engineering: Neue Angriffsmethode richtet sich gegen Firmen

20.01.2017 - In den letzten Tagen wurden der Melde- und Analysestelle Informationssicherung MELANI mehrere Fälle gemeldet, bei denen Betrüger Firmen anrufen, sich als Bank ausgeben und behaupten, dass am nächsten Tag ein E-Banking-Update durchgeführt würde. Sie verlangen, dass an diesem Termin verschiedene Mitarbeitende der Finanzabteilung anwesend sind. Dies hat den Zweck, das Sicherheitselement «Kollektivunterschrift» auszuhebeln und so eine betrügerische Zahlung auszulösen.

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

8.3 Checklist and instructions

In the first half of 2017, MELANI did not publish any new checklists or instructions.

9 Glossary

Term	Description
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.
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").
Border Gateway Protocol	Border Gateway Protocol is the routing protocol used on the internet. It connects up autonomous systems.
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.
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.
Content delivery network	A content delivery network is a network of regional distributors and servers connected via the internet through which content, in particular large media files, are delivered.

Cyber-blurring strategy	Cyber-blurring describes the method of placing targeted inaccurate data in a dataset so as to hamper the work of the attackers.
Data URL	A data URL is a URI scheme which allows data in (HTML) source text to be embedded as though it were external resources.
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 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).
DriveBy-Infection	Infection of a computer with malware simply by visiting a website. Often the websites concerned contain reputable offerings and have already been compromised beforehand for the purposes of spreading the malware. The infection occurs mostly by trying out exploits for vulnerabilities not yet patched by the visitor.
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.
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.
Ethernet	Ethernet is a technology for wired data networks.
Exploit-Kit	Toolkits with which criminals can generate programs, script or lines of code to exploit vulnerabilities in computer systems.
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.

IP-Address	Address to uniquely identify computers on the Internet or on a TCP/IP-network (e.g.: 172.16.54.87).
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.
Launcher	A computer program which helps to locate a program and launch it.
Malicious code	Generic term for software which carries out harmful functions on a computer, e.g. viruses, worms, Trojan horses.
Malware	Generic term for software which carries out harmful functions on a computer, e.g. viruses, worms, Trojan horses.
Managed service providers (MSP)	A managed services provider (MSP) is an information technology service provider which assumes the responsibility for the provision of a defined series of services for its client and manages these services.
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.
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.
Plug-in	A plug-in is an optional software module that extends or changes existing software.
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.
RAM	Random-access memory (RAM) is a data storage system which is used particularly in computers for data storage that is usually in the form of memory modules.
Remote Administration Tool	A remote administration tool is used for the remote administration of any number of computers or computing systems.
RootKit	A collection of programs and technologies which allow unnoticed access to and control of a computer to occur.
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.
Smartphone	A smartphone is a mobile phone that offers more computer functionality and connectivity than a standard advanced mobile phone.
SMB protocol	Server message block (SMB) is a network protocol for file, printing and other server services in computer networks.
SMS	Short Message Service for sending text messages (160 characters maximum) to mobile phone users.
Social Engineering	Social engineering attacks take advantage of people's helpfulness, credulity or lack of self confidence in order to gain access to confidential data or to prompt them to perform certain actions, for example.
Software defined radio	The term software defined radio (SDR) refers to concepts for high-frequency transmitters and receivers where smaller and bigger sections of signal processing is realised with software.
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.
SSH	Secure Shell A protocol for encrypted communication. It may be used to securely login to a computer system via a network (e.g. the Internet).
Subscription bomb	Subscription bomb refers to the organised registering of email addresses with newsletter providers to block the inboxes or the communication facilities of the recipient.
Take-down	Expression used when a provider takes down a site from the network due to its fraudulent content.
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.)
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).
Vulnerability	A loophole or bug in hardware or software through which attackers can access a system.
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.
Win32PE file	Portable executable (PE) describes a binary format executable program. It is the file format which is used in Win32 and Win64 systems for executable files.
WLAN	WLAN stands for Wireless Local Area Network.
Zero-Day	An exploit which appears on the same day as the securi-

	ty holes are made public.
ZIP-File	zip is an algorithm and file format for data compression, in order to reduce the storage space needed for the archiving and transfer of files.