Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal IT Steering Unit FITSU
Federal Intelligence Service FIS

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

INFORMATION ASSURANCE

SITUATION IN SWITZERLAND AND INTERNATIONALLY

Semi-annual report 2016/I (January – June)

28 OCTOBER 2016

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

1 Overview/content

1 Overview/content 2
2 Editorial 5
3 Key topic: Cyberextortion – Cybercrime trend 6
3.1 The recipe for success 6
3.2 Dynamics of the criminal ecosystem 6
3.3 Success inspires copycats 7
4 Situation in Switzerland 8
4.1 Espionage 8
4.1.1 Turla at a defence company 8
4.2 Data leaks 11
4.2.1 Predictable router passwords 11
4.2.2 Passwords of 6,000 Swiss email accounts in circulation 12
4.2.3 Database of the Swiss People's Party hacked 12
4.3 Industrial control systems 13
4.3.1 Failure of payment terminals 13
4.3.2 Internet breakdown for business clients 13
4.3.3 Arson attack on the SBB's cable duct 13
4.4 Attacks 14
4.4.1 DDoS and extortion 14
4.4.2 Infection on 20min.ch 16
4.4.3 OpnessunDorma by Anonymous against job websites in Ticino and Italy 17
4.4.4 Hackers at the Federal Institute of Technology 18
4.5 Social engineering, phishing 18
4.5.1 Phishing statistics 18
4.5.2 Perfected CEO fraud persists 19
4.6 Crimeware 20
4.6.1 Increase in malicious Android apps in Switzerland 21
4.6.2 Bogus summons leads to encryption Trojan 22
4.6.3 Unsolicited job applications with ransomware 22
4.6.4 Encryption Trojans – technical aspects 23
4.7 Preventive measures 25
4.7.1 First MELANI awareness day: Ransomwareday 25
5 Situation internationally 25
5.1 Espionage 25
5.1.1 Espionage attack interferes with election campaign 25
5.2 Data leaks 26

5.2.1 Unwanted publication of electoral registers 26
5.2.2 What users did not want to share with their professional network 26
5.2.3 Twitter access data on the black market 27
5.3 Industrial control systems 27
5.3.1 Malware in a German nuclear power plant 27
5.3.2 Publication about a cyberattack on a water company 28
5.3.3 New type of malware with clear connection to ICS but unclear target 29
5.3.4 US government and car manufacturers agree on safety cooperation 30
5.3.5 Car theft using electronics 30
5.4 Attacks 31
5.4.1 Cyber bank robbers steal USD 81 million 31
5.4.2 Carbanak 2.0 and similar attacks 32
5.4.3 Ransomware in hospitals 33
5.4.4 Japanese ATMs looted 34
5.4.5 Anonymous & Co: #campaigns 34
5.4.6 xDedic: buying access to hacked services in online shops 35
5.5 Preventive measures 36
5.5.1 Raid on the darknet 36
5.5.2 Angler and Nuclear exploit kit activity subsides 37
5.5.3 Several arrests of Dyre instigators in several countries 38
6 Trends and outlook 38
6.1 Highly developed attacks – criminals now also an APT 38
6.2 The future of the internet – from a technological and social perspective 39
7 Politics, research, policy 41
7.1 Switzerland: Parliamentary procedural requests 41
7.2 EU: Directive on security of network and information systems (NIS Directive) 43
7.3 France: new rules for critical infrastructures 43
8 Published MELANI products 45
8.1 GovCERT.ch Blog 45
8.1.1 SMS spam run targeting Android Users in Switzerland 45
8.1.2 Dridex targeting Swiss Internet Users 45
8.1.3 Technical Report about the RUAG espionage case 45
8.1.4 20min.ch Malvertising Incident 45
8.1.5 Leaked Mail Accounts 46
8.1.6 Armada Collective is back, extorting Financial Institutions in Switzerland 46
8.1.7 Gozi ISFB - When A Bug Really Is A Feature 46
8.1.8 TorrentLocker Ransomware targeting Swiss Internet Users 46

8.2 MELANI Newsletter 46
8.2.1 Offline Zahlungs-Software im Visier von Hackern - Schweizer Unternehmen betroffen 46
8.2.2 Vermehrt schädliche Office Dokumente im Umlauf 47
8.2.3 Technical Report about the Malware used in the Cyberespionage against RUAG 47
8.2.4 Swiss Ransomware Awareness Day 47
8.2.5 Handling security bugs, vulnerable infrastructure and a range of DDoS attacks: 22nd MELANI semi-annual report 47
8.2.6 Passwörter von 6'000 E-Mail-Konten im Umlauf 48
8.2.7 Betrügerische Telefonanrufe gegen KMUs im Zusammenhang mit dem eBanking Trojaner „Retefe" 48
8.3 Checklists and instructions 48
9 Glossary 48

2 Editorial

Martin Sibler has worked in different areas of information assurance at Swiss Re since 2001

Dear reader,

For the insurance industry, information is a key element of the value chain. Assessing insurable risks requires mathematical formulae as well as historical information about the event – such as a hurricane in Florida – in order to calculate the probability of occurrence. Additionally, information provided by clients – such as the location of the building to be insured – is often included in the analysis. The integrity, confidentiality and availability of this information must be ensured. Availability of the right information at the right time makes it possible to understand the risk better and, to a certain extent, to predict it.

The starting point for assessing cyber risks is similar, but there are numerous dynamic factors that make it more difficult to gauge the risk. Firstly, the information about earlier events is not very extensive, and secondly, this information is often no longer relevant, because the technology and the types of attack have changed in the meantime. For hurricanes, the parameters are always about the same: the wind force varies and the path of destruction changes, but there are many records of hurricanes that can be taken into account. For an event in cyberspace, not only do the wind force and the path change, but the hurricane may even suddenly turn out to be an earthquake. The comparison may not be perfect, but it does show that one should expect the unexpected when dealing with cyber risks. Information on hacker attacks over the past 20 years is only of limited help in gauging the threat situation.

For this reason, cyber intelligence – i.e. timely exchange of information about current attacks – is especially helpful for assessing whether to protect oneself from a hurricane or from an earthquake. MELANI offers an important service in this regard, helping the Swiss economy improve how it protects itself from such risks.

I hope you enjoy reading this report,

Martin Sibler

3 Key topic: Cyberextortion – Cybercrime trend

Cryptolocker, Armada Collective, Rex Mundi: What do all these threats in the headlines have in common? They are all instances of cyberextortion! This profitable scam has been very popular among criminals for several years. Instead of stealing money directly, the victim is put under pressure in some way and made to pay a ransom. The most recent developments of these attack methods are discussed in chapters 4.6.2 and 4.6.3 (ransomware) and 4.4.1 (DDoS and extortion) of this semi-annual report. But first, let's take a look at the reasons for the success and rapid development of these methods.

3.1 The recipe for success

These methods offer many advantages for perpetrators: The attacks are not limited to systems used to manage or process money. The circle of potential targets is thus enormously greater and nearly unlimited. In principle, attackers may target all data or systems that are of value to a user or company and important enough that the victim is willing to pay a ransom to get them back. This modus operandi also has the advantage for criminals that they receive the money in a much simpler and anonymous way, no longer requiring that the money be laundered using third parties. Criminals demand payment directly in the currency of their choice – i.e. that is hardest to trace. It is thus no coincidence that these methods have been gaining ground rapidly since the emergence of new means of payment such as bitcoin and the like, which can be used to conceal the identity of the recipient. Through anonymisation, criminals make it nearly impossible to identify the recipients of bitcoin payments.

The development of these extortion attacks is characteristic of the approach taken by perpetrator groups currently active on the internet. The prevalent entrepreneurial approach often moves between opportunism, efficiency optimisation and adaptability. As long as an attack pattern is profitable, it is maintained and further developed. Ransomware impressively illustrates this development. Although its mode of operation has been well-known for several years, ransomware continues to develop in numerous variants and is being endowed with even more effective features. The vicious circle is that the more money these criminal enterprises extort from their victims, the more resources they have to finance their infrastructure and advance research and development. With these improvements, they become even more efficient and, despite steadily improving protective measures, they are able to extort a sufficiently high number of new victims.

3.2 Dynamics of the criminal ecosystem

The criminals' dynamics and their search for efficiency is ultimately no different from what we know of any profit-maximising enterprise. Firstly, the criminals must make sure that their technology is more advanced than that of security service providers. A cornerstone of any criminal enterprise engaged in ransomware is the availability of encryption methods that cannot be cracked. For this purpose, the criminals must always monitor developments relating to their software and improve it immediately if someone is able to circumvent their encryption. Secondly, the criminals must continuously try to expand their base of customers (i.e. of potential victims). This is done mainly by improving the methods used to infect victims. For instance, infected emails are used to trick spam filters by being sent from the compromised account of a victim's contact or in the name of a public authority. New compromising methods are also being observed: in some cases, ransomware has been smuggled in using RDP (Remote Desktop Protocol for remote access to Windows servers) that had previously

been compromised using a brute force attack. At the same time, criminals try to expand their victim base by, for instance, encrypting not only the data of users and companies, but rather also website content directly. Attacks are also being optimised by selecting targets with dramatic consequences when data is no longer accessible. Logically, this increases the willingness to pay a ransom. This includes the observed attacks against hospitals. With the internet of things and the actual networking – rather than merely connecting – of numerous devices, the range of applications for ransomware appears unlimited. Once a system has been compromised, the goal is to extort as much profit as possible. Like in the business world, criminals practice a "customer-oriented" approach. They use direct channels (live chats) to communicate with their victims and to explain the best way to pay ransom money. They also look for ways to increase the pressure on victims, not limiting themselves to making data unreadable, but also threatening to publish sensitive data.

3.3 Success inspires copycats

These attacks are so profitable that they inspire numerous copycats. Encryption Trojans meanwhile exist in innumerable versions. But these dynamics can also be observed for other types of cyberextortion such as DDoS attacks. A giant array of attackers with a wide range of capabilities has emerged in the field of DDoS. This includes numerous copycats who imitate the approach taken by the original perpetrators. They are aided not least of all by the fact that DDoS attacks can meanwhile be bought without major effort from an "attack service" (booter, stresser). Recently, most active attackers have been pure opportunists. They are riding the wave of attacks and sending out extortion emails without bothering to launch a real attack, which they most probably would not even be capable of anyway. They purport to be groups (such as Armada Collective) that have become known through the media, hoping that the fear of an attack is enough to make victims pay.

This means we are confronted with an extremely profitable extortion market attracting a wide range of perpetrators, some of whom demonstrate considerable ingenuity. It must therefore be feared that these attacks will persist and continuously be further developed. Ultimately, however, the whole market rests on the assumption that a critical mass of victims is willing to pay a ransom so that these groups make enough profit and are able to finance their activities. Without this source of financing, the system implodes. It can therefore not be overemphasised how important it is not to give in to these extortions. But that is not enough. At the same time, information must always be provided on how to protect oneself from these attacks. Every company must deal with this threat and ask itself what information and which systems are so sensitive that they may become the object of extortion, what methods may be used to gain access to the data or systems, how they can be protected and whether there are procedures for responding to an extortion attack. Users and companies that are not sufficiently prepared for such contingencies will unfortunately fall for the extortion and pay a ransom.

Recommendation:

MELANI makes numerous documents available on how to protect against threats:

DOKU

Measures to counter DDoS attacks
https://www.melani.admin.ch/melani/en/home/dokumentation/checklists-and-instructions/massnahmen-gegen-ddos-attacken.html

DOKU

Measures to counter ransomware
https://www.melani.admin.ch/melani/de/home/themen/Ransomware.html

4 Situation in Switzerland

4.1 Espionage

4.1.1 Turla at a defence company

On 4 May 2016, the Federal Department of Defence, Civil Protection and Sport (DDPS) published a media release,[1] according to which the Federal Intelligence Service (FIS) had informed the Office of the Attorney General in January 2016 that computers of the defence company RUAG had been infected with espionage software. On 25 January 2016, the Office of the Attorney General initiated a criminal investigation against persons unknown. Media interest was great in the wake of this media release, and the political treatment of the case is not yet concluded. On behalf of the Federal Council, the Reporting and Analysis Centre for Information Assurance (MELANI) published a report with the technical findings in the RUAG case on 23 May 2016. This measure aimed to give other companies the opportunity to check their networks and take appropriate protective measures.[2,3]

The attackers used malware of the "Turla" Trojan type, which has been in circulation for several years already. While the version observed in the RUAG network did not have any *rootkit* functionality, it did disguise itself in order to avoid detection. The attackers showed a lot of patience when infiltrating and further penetrating the network. They attacked only targets they were interested in.

An important intermediate target of the attack was the *active directory*. Once it has accessed this central address book, the Trojan can further access other applications and devices con-

1 https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-61618.html (as at 31 August 2016).

2 https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-61788.html (as at 31 August 2016).

3 https://www.melani.admin.ch/melani/en/home/dokumentation/reports/technical-reports/technical-report_apt_case_ruag.html (as at 31 August 2016).

taining interesting data by setting appropriate authorisations and group memberships. To hide the communication to the extent possible, the malware used the http protocol for data transfer to several *command & control servers*. These control servers in turn sent tasks to the infected devices, such as to download new binary or configuration files or *batch jobs*. A hierarchical system was used: with this architecture, not every infected device communicates with the control servers, but rather the work is divided up. Some systems called "communication drones" are responsible for communicating with the outside world. Other "worker drones" are used solely to steal and pass on data to the communication drones.

It is difficult to assess the effective damage, and doing so was not part of the RUAG report published by MELANI or of this report. The analysis of the *proxy logs*, however, showed that data was not being read at all times. There were phases with very low level of activity in terms of both queries and data volumes, but also phases with a high number of queries and large data leaks.

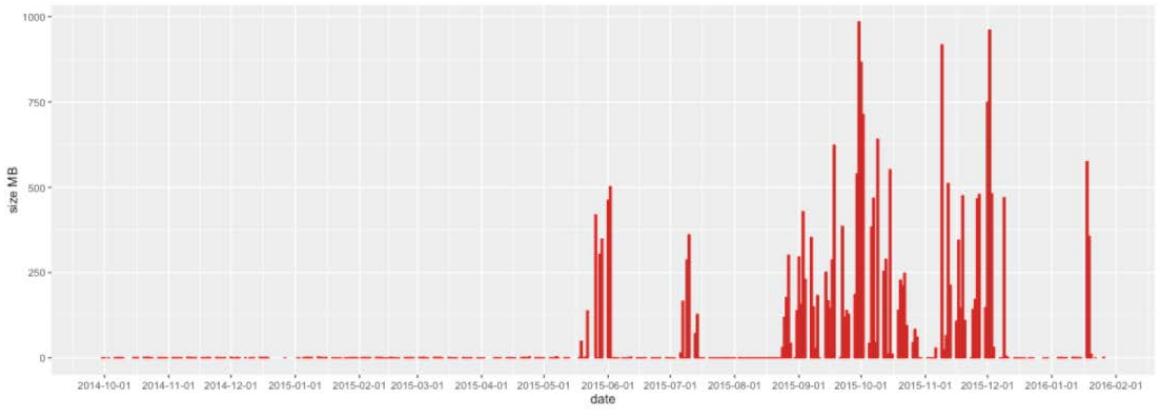


Figure 1: Data leak volume per day

Complete protection from such sophisticated attacks is difficult to achieve. Many countermeasures are not very expensive, however, and can be implemented with a reasonable amount of effort. Especially when an attacker makes a mistake, incidents can in fact be detected. For that purpose, employees' awareness must be raised so that they can recognise and properly interpret malfunctions and suspicious behaviour in the systems, and so that they can respond accordingly. A list of such measures is included in the MELANI/GovCERT RUAG report[4] starting on page 27.

Awareness must also be raised for the importance of exchanging experiences and information with other companies, the economic sector in question, or the Federal Administration. MELANI's "closed constituency" now includes more than 190 companies operating critical infrastructure and is an important vessel for exchanging such information among companies, even anonymously where necessary. MELANI's international network also makes an important contribution to recognising attacks, given that cyber incidents do not stop at borders. Every day, numerous leads are received from Switzerland and abroad that might lead to a breakthrough. As part of its responsibilities and the National Strategy for the Protection of Switzerland against Cyber Risks (NCS), MELANI promotes information exchange among operators of critical infrastructures, so that targeted attacks will continue to be detected in the future and thwarted where possible.

[4] https://www.melani.admin.ch/melani/en/home/dokumentation/reports/technical-reports/technical-report_apt_case_ruag.html (as at 31 August 2016).

For an overview of the case, the incidents are presented chronologically in the figure below:

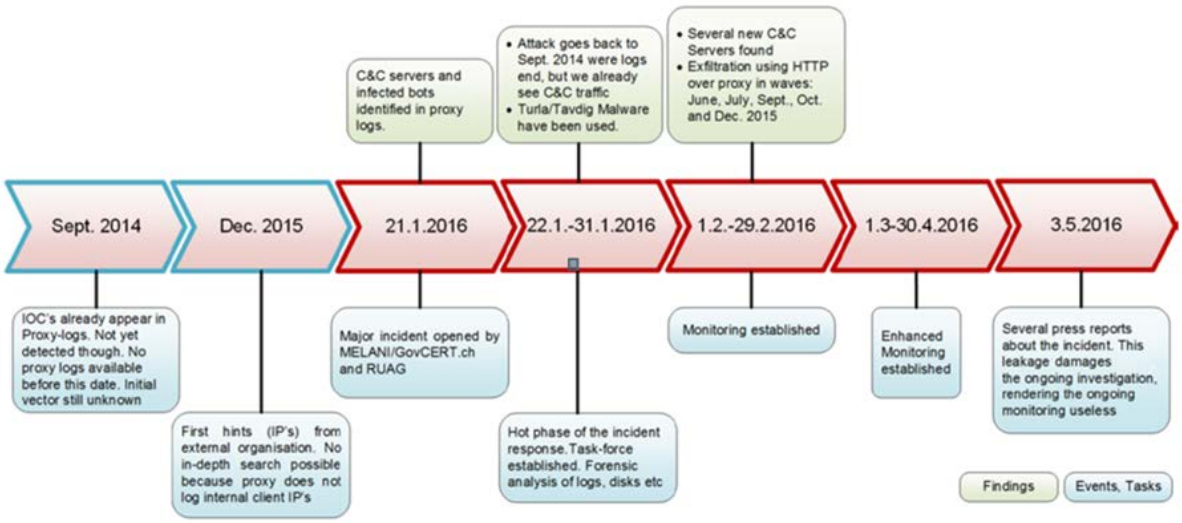


Figure 2: Chronology of the response to the attack

Conclusion/recommendation:

Cyber espionage is a reality. In past MELANI semi-annual reports, we have already reported on several cases. The annual report of the Federal Intelligence Service (FIS) also considers this issue. Prevention is an extremely important component of the fight against cyber espionage. The first and most important step for an enterprise is the realisation that cyber espionage is a real threat, not a hypothetical one. Numerous cases known to MELANI confirm this. To combat espionage efficiently, the flow of information must also be ensured. If espionage cases are reported, the authorities can take measures and summarise the findings for decision-makers in politics and business. Finally, this information helps other organisations detect possible attacks against their systems. For the authorities, it is of course a top priority to treat the information confidentially.

In partnership with the private sector, MELANI has worked for 12 years on protecting against IT threats. For reporting incidents relating to information assurance, MELANI makes a reporting form available on its website:

MELANI reporting form:

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

In its Prophylax programme, the Federal Intelligence Service (FIS) carries out a prevention and awareness-raising campaign in the field of non-proliferation and economic espionage. It serves to raise the awareness of enterprises and educational institutions:

Prophylax programme:

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

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

4.2 Data leaks

4.2.1 Predictable router passwords

UPC *Routers* are delivered with a factory-set password. The *WLAN* name (the so called *SSID*) contains a random seven-digit number. This password is individually generated by the manufacturer for each router and looks random. In a publication which appeared on the internet at the end of last year, it was possible for unauthorized persons to guess this predefined standard password. Users, who have changed the password from the start, were of course not affected. For certain UPC devices, this tool makes it possible to calculate a selection of 8 to 12 passwords for the *WPA2 key* using the *WLAN* name. In addition to this tool, which was intended mainly for experts, the discoverer of this security vulnerability put an online tool on the internet a few days later that anyone can use very easily. With this action, the discoverer of the vulnerability wanted to show that certain manufacturers are neglecting security when generating passwords. The exploited vulnerability was not really new: It is

based on a research paper from the Netherlands that was published already in spring 2015 and presented at a security conference in Las Vegas in summer 2015.

At the beginning of July 2016, the story repeated itself. This time, the incident concerned the Ubee EVW3226 router, which is also used in Switzerland. In this case, the *MAC address* of the device – not the SSID – was needed to calculate the passwords. The MAC address can be determined quite easily using various tools within the wireless range of a WLAN network. In this case, it was possible to use the information to calculate the correlating factory-set standard passwords and SSIDs. Also in this case only users were affected, who haven't changed right from the start their password as recommended.

Conclusion/recommendation:

The use of standard passwords should be avoided in any case, especially if the devices are accessed from the internet or a wireless signal. Many manufacturers have responded to this by using a custom factory-set password instead of the usual "123456" combination. It is all the more unfortunate if this custom factory-set password can be calculated by third parties, resulting in a security vulnerability. The rule therefore continues to apply that the password should be changed in any case as soon as the device is put into operation and before it is connected to the internet. Most devices offer a reset function if the user forgets the password. But this requires the user to be physically present in most cases to push the reset button on the device. It is recommended to change the standard passwords individually as in many other devices or logins. At one hand this is more secure but also easier to handle in the daily business.

4.2.2 Passwords of 6,000 Swiss email accounts in circulation

On 16 March 2016, MELANI was forwarded 6,000 hacked email/password combinations that had been stolen by hackers. These accounts could have been misused for illegal purposes such as fraud, extortion, phishing, etc., if the users did not immediately change the passwords. For that reason, MELANI published an online tool for checking whether one's email address had been hacked. Entering the email address was sufficient to use the tool. The email address was encrypted before being sent and was also not stored.

Most of the responses to these efforts were positive. However, there were some critical voices expressing concern whether the site was really legitimate and set up by MELANI. In terms of raising awareness and prevention, this response is welcome. Healthy scepticism is appropriate in such cases, and it is certainly a good idea to double-check whether a site is legitimate. In this case, MELANI believed that a fast publication of the online tool was the most practicable and efficient way to offer potentially affected users the opportunity to perform a check.

4.2.3 Database of the Swiss People's Party hacked

During an attack on a database of the Swiss People's Party in mid-March 2016, about 50,000 email addresses were copied. A group calling itself "NSHC" claimed responsibility for the attack. According to a statement given by NSHC to the online journal inside-channels.ch, the

group wanted to show that Switzerland was not sufficiently protected against cyberattacks.[5] The group referred to itself as "*grey hats*", i.e. hackers who may not obey the law, but who do not intend to cause direct damage. At the same time, the group claimed responsibility for the *DDoS* attacks against Interdiscount, Microspot, and the Swiss Federal Railways (SBB), which also took place that week. Here again, the group said its motive was a wake-up call for IT security officers. It is not known whether the group actually has DDoS capacities or simply wanted to jump on the bandwagon of the surge in DDoS attacks in March. The NSHC group had been unknown previously and also wasn't observed afterwards.

4.3 Industrial control systems

If a website or online service is down nowadays, the inevitable suspicion is that the cause is a hacker attack. But technical faults are still among the main reasons for breakdowns of industrial control systems. This can be seen impressively in the following event, even though it took place quite some time ago: On 22 June 2005, the power grid of the Swiss Federal Railways (SBB) broke down because two out of three transalpine power lines were interrupted due to construction work and the transmission capacity of the third line had been overestimated. This resulted in a safety shutdown of the third line and a separation of the power grids north of the Alps and south of the Alps. While the events in the first half of 2016 did not reach this magnitude, the effects were still serious and demonstrated the dependency of modern means of communication.

4.3.1 Failure of payment terminals

On 20 June 2016, cashless payments were disrupted. In all regions of Switzerland and even Austria, service providers were affected who used a *payment terminal* operated by the financial service provider SIX. However, the problem was neither ubiquitous nor consistent. This made it difficult to find the error. It turned out that an error at the network level was responsible.

4.3.2 Internet breakdown for business clients

Swisscom struggled with problems a month earlier. The internet for business clients was hit by a massive failure. At noon on 24 May 2016, the internet broke down for numerous clients. At times, even ATMs were affected. The breakdown was finally identified as a problem with Swisscom's Ethernet Access Platform in the Lausanne region.

4.3.3 Arson attack on the SBB's cable duct

In contrast, the cause of the breakdown of one of the important railway connections to Zurich Airport was a physical attack in the Zürich-Oerlikon area. Unknown perpetrators lit fires in two cable channels running parallel to the tracks in the early morning of 7 June 2016. The repair of the burnt cables required laborious manual work. The rail operation in the area Oerlikon – Zurich Airport was heavily impacted. The line to the airport remained interrupted until the evening.

[5] http://www.inside-it.ch/articles/43272 (as at 31 August 2016).

Conclusion:

Alongside the risk of electronic attacks, the risk of physical attacks on electronic systems should not be ignored. Power and telecommunications cables in particular can be protected only partially across long stretches. While physical attacks generally have only a local impact, the protection especially of neuralgic points and systems should not be limited to the electronic level, but should also include the physical level.

4.4 Attacks

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

4.4.1 DDoS and extortion

Cyberextortion is the key topic of this report. This chapter discusses the development of extortion combined with DDoS threats. We have already reported on groups like DD4BC and Armada Collective (Semi-annual reports 2015/1 and 2015/2). These perpetrators used the method that is meanwhile well-known and well-documented: after an initial DDoS attack for purposes of demonstration, the attackers extort the victim. If a bitcoin payment is not made by a certain deadline, a second attack more intense than the first is threatened.

This year began with a success story in law enforcement: in January 2016, Europol announced that two DD4BC members had been arrested.[6] Since then, there have been no observed attacks in the name of Armada Collective or DD4BC using the "original" method described above. This may support the thesis that Armada Collective and DD4BC are in fact the same group and that the most important heads are now behind bars.

[6] https://www.europol.europa.eu/content/international-action-against-dd4bc-cybercriminal-group (as at 31 August 2016).

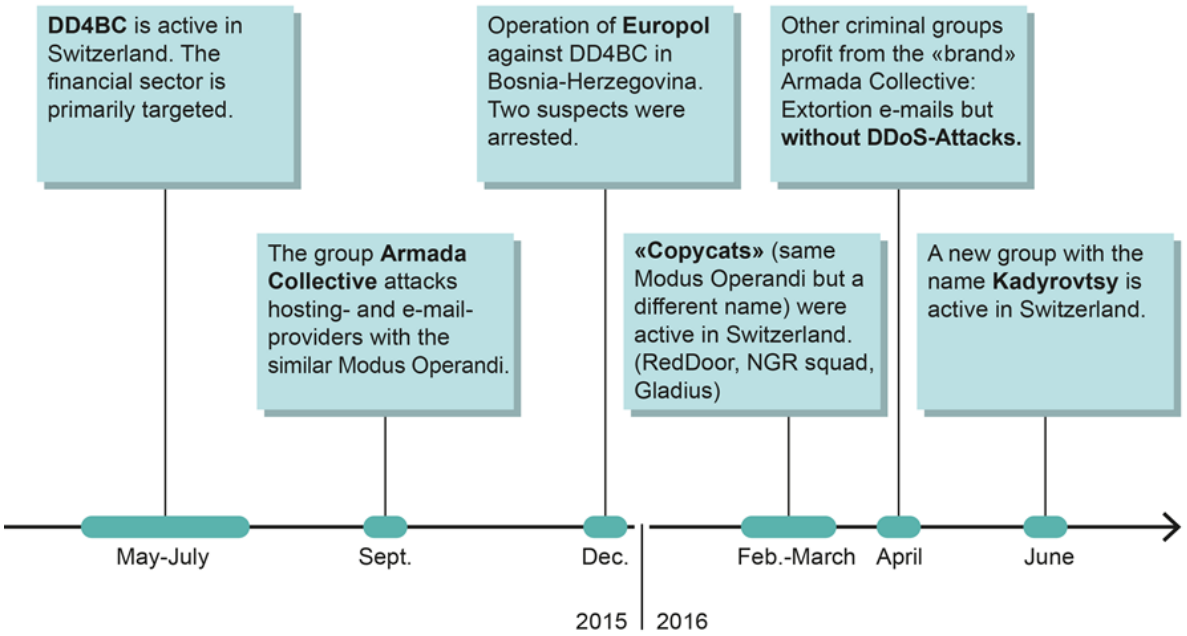


Figure 3: DDoS et extorsion : timeline

The threat situation has changed since the arrest. Other groups have emerged in the meantime that use parts of this modus operandi. Several groups of perpetrators have carried out attacks using the typical DD4BC/Armada pattern – DDoS attacks for purposes of demonstration followed by extortion. These groups are copycats. They operated between March and June under the names of RedDoor, NGR Squad, Gladius and Kadyrovtsy. In the first half of the year, the most striking development was the emergence of opportunists who sent out numerous extortion emails with DDoS threats under the name of Armada Collective. In these cases, however, no attacks took place, even for demonstration purposes. The groups extorted money merely by exploiting the fear of Armada Collective that had arisen after reports about that group's activities. Typical in these cases was that all victims were given the same bitcoin address for making the ransom payment. This means the attackers wouldn't even have been able to figure out who paid and who didn't and thus who should be attacked. Moreover, numerous threats were made at the same time on the same day, which would have required enormous DDoS capacity for the attackers. In such cases, it is highly probable that this is the work of an opportunist. Amusingly, a person claiming to be Armada Collective complained to MELANI about misuse of the Armada Collective brand:

> I'm member of original Armada Collective and I have just noticed your report on Twitter. Armada Collective is dead. We have stopped all operations, because it wasn't profitable enough and risk was too big. When I realized that somebody is using our name I got mad. It is obviously an amateur copycat using our name who copied our text (maybe from your site) and is probably not even capable of launching DDoS attacks. Good luck with your investigation.

Figure 4: Message received by MELANI via reporting form

The increase of the various activities shows how profitable extortion is for criminals. Criminals rely not only on specific attacks, but also on mere fear of such attacks. In light of these dynamics, it is difficult to gauge to what extent reports with precise information on the approaches taken by perpetrators serve as a source of inspiration. In our view, it is important to report on the approaches taken. But it cannot be ruled out that such publications inspire copycats or provide a platform for attackers to profit from their newly gained public notoriety.

On the other hand, cases in which many companies have simultaneously received extortion emails show how important it is to exchange information about such events and to report on them. Thanks to reporting to a central authority such as MELANI, an overview of comparable cases can be established and the situation can be assessed more effectively. In this connection, information about the provided bitcoin address or data concerning the strength of the attack are of immense importance. It should also be recalled that protection from DDoS attacks – a type of attack that different criminals may use for different purposes – must continue to be given a high priority.

Recommendation:

If a DDoS attack hits a company unprepared, fast and efficient countermeasures are hardly possible anymore. In enterprises heavily dependent on online sales, securing this highly critical business process must be given absolute priority. For that reason, a strategy for the event of a DDoS attack must be developed. The internal and external contact points as well as other persons able to respond in the event of an attack must be known. Ideally, the senior management of a company should deal with the DDoS threat already before an attack as part of general risk management, and certain DDoS countermeasures should be established throughout the enterprise. A DDoS attack can affect any organisation. Talk to your internet provider about your needs and appropriate precautions. A checklist and instructions with measures against DDoS attacks can be found on the MELANI website:

Checklist and instructions with measures against DDoS attacks:

https://www.melani.admin.ch/melani/en/home/dokumentation/checklists-and-instructions/massnahmen-gegen-ddos-attacken.html

4.4.2 Infection on 20min.ch[7]

Already in the previous half-year, the e-banking Trojan Gozi ISFB was spread via various news websites of the Tamedia group. The last MELANI semi-annual report discussed this.[8] At the beginning of April of this year, the incident happened again – this time on the website of the free newspaper "20 Minuten", which also belongs to the Tamedia group. The Federal Administration and several companies temporarily blocked access to the 20min.ch website starting on 7 April. Tamedia was informed of this measure. The source of the incident discovered by MELANI was a *JavaScript* inserted into a multimedia file (*SWF animation file*) on the website. The script was launched when the website was visited, leading the visitor to the Niteris *exploit kit*, which automatically downloaded the Gozi Trojan to the computer of the

[7] http://www.srf.ch/news/schweiz/nach-malware-attacke-auf-20-minuten-was-sie-jetzt-tun-koennen
http://www.20min.ch/digital/news/story/20minuten-ch-erneut-Ziel-von-Malware-Attacke-15457508
http://www.nzz.ch/digital/malware-auf-20minch-tamedia-gab-zu-frueh-entwarnung-ld.12431
http://www.tagesanzeiger.ch/digital/internet/Erneut-ein-Trojaner-auf-20minutench/story/19684342 (as at 31 August 2016).

[8] MELANI Semi-annual report 2015/II, chapter 4.3.1.1
https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2015-2.html (as at 31 August 2016).

victim. After the website had been cleaned, it was attacked again just a few days later. In that later incident, however, it was not the website of 20 Minuten itself that was affected, but rather the network of an external advertisement provider whose advertising windows were built into the 20 Minuten website. The Bedep malware was spread using the known Angler exploit kit. This exploit kit was also used for similar attacks on the nytimes.com and bbc.com websites.[9] Electronic daily newspapers are clicked on every day by millions of visitors. They are therefore ideal for drive-by download attacks. This approach has been observed increasingly in Switzerland since spring 2015.[10] According to 20 Minuten, the company's own servers are attacked between 20 and 50 times a day.[11]

Recommendation:

To avoid such infections on the side of end users, operating systems and applications must be updated regularly – and if possible automatically. Restrict the execution of JavaScripts (Active Scripting) in your browser settings or with the help of add-ons to the extent possible, or disable JavaScript entirely. If you disable JavaScript, however, you should note that many websites will no longer work properly. If this interferes too much with your web browsing, ease the restrictions (step by step) to an acceptable level. Depending on the method used, it is also possible to define certain websites where JavaScript is allowed (whitelisting).

If you suspect your computer has been infected, consult an expert who will examine your computer and either clean it or re-install it as necessary.

INFO

Rules of Conduct ➔ Surfing:

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

4.4.3 OpnessunDorma by Anonymous against job websites in Ticino and Italy

37 Italian job websites and seven in other countries (including four in Ticino) were the victims of a cyberattack between 9 and 11 April 2016. The company websites were defaced, and millions of datasets were stolen. Anonymous Italia and LulzSecITA claimed responsibility for the attack. They published the login data of users as well as information on the structure of various databases and the document names of several thousand curricula vitae (the curricula vitae themselves were not published, however). The groups cited two reasons for the attack: firstly, they wanted to show that "job placement services exploit employees like parasites". Secondly, the attackers wanted to uncover the vulnerability and poor security of IT platforms

[9] http://www.nzz.ch/digital/newssite-gesperrt-mittels-20minch-malware-verbreitet-ld.12263 (as at 31 August 2016).

[10] https://www.govcert.admin.ch/blog/21/20min.ch-malvertising-incident (as at 31 August 2016). https://www.govcert.admin.ch/blog/13/swiss-advertising-network-compromised-and-distributing-a-trojan https://www.govcert.admin.ch/blog/18/gozi-isfb-when-a-bug-really-is-a-feature (as at 31 August 2016).

[11] http://www.20min.ch/digital/news/story/Keine-Gefahr-fuer-die-Nutzer-der-20-Min-App-10440966 (as at 31 August 2016).

on which user data is stored.[12] ticinoonline.ch published a screenshot of the defaced website of e-lavoro.ch – the website of the Association of Ticino's Industries (Associazione industrie Ticinesi AITI) – which had been affected by the attack along with BFKconsulting.ch, helvia.com and workandwork.ch.[13] On that screenshot, the Ticino victims are accused of subordinating themselves to the "xenophobic and racist right-wing laws in Switzerland" and of publishing job advertisements that are addressed only to residents of Switzerland.[14]

4.4.4 Hackers at the Federal Institute of Technology

In January 2016, a perpetrator logged onto the network of the Swiss Federal Institute of Technology Zurich (ETH Zurich) for several days using someone else's access data, ordering software via the ETH system and downloading sensitive data. Once the ETH detected the misuse of its network, the public prosecutor of the Zurich Competence Centre for Cybercrime was contacted, who together with police investigators immediately initiated urgent safety measures and pushed the investigations forward. The alleged perpetrator was arrested already ten days after the investigation commenced. The accused is now in pretrial detention. Criminal proceedings were initiated on charges of unauthorised access to a data processing system and unauthorised data gathering.[15]

4.5 Social engineering, phishing

Apart from all of the technical attacks, methods that exploit human weaknesses are also popular with attackers.

4.5.1 Phishing statistics

In recent years, the number of *phishing* enquiries received by MELANI has risen dramatically. To process the large number of phishing reports more efficiently, MELANI launched the antiphishing.ch website in 2015, which can be used to report phishing sites. In total, 2,343 phishing unique sites were reported on antiphishing.ch in the first half of 2016. Figure 5 shows the number of phishing sites reported each week. The number fluctuates over time. The reasons vary: firstly, some of the fluctuations are due to holidays, since fewer phishing sites are reported during holidays; secondly, attackers regularly shift their attacks from country to country.

---

12 https://share.cyberguerrilla.info/?3263d9dcba87924c#nxVUhZU/s/diAc9ZJ1v+cjkH1F+oT3K+iiljOHLLT+0= (as at 31 August 2016).

13 http://www.rsi.ch/news/ticino-e-grigioni-e-insubria/Siti-ticinesi-hackerati-7176668.html (as at 31 August 2016).
http://www.radiondadurto.org/2016/04/12/anonymous-italia-operazione-nessundorma-e-la-violazione-della-legge-sulla-privacy/ (as at 31 August 2016).
http://www.tio.ch/News/Ticino/Cronaca/1079978/Attacco-hacker-colpiti-4-siti-ticinesi--Rubati-milioni-di-dati/ (as at 31 August 2016).

14 One corporate group is mentioned in particular, operating in the production and sale of orthopaedic prosthetics.

15 https://www.ethz.ch/de/news-und-veranstaltungen/eth-news/news/2016/02/mm-mutmasslicher-hacker-verhaftet.html (as at 31 August 2016).

Figure 5: Reported and confirmed phishing sites per week at antiphishing.ch

4.5.2 Perfected CEO fraud persists

CEO fraud – this method has already been discussed several times by MELANI in newsletters and semi-annual reports. 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 compromised real 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 often also 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.

Several cases abroad made headlines in the first half of 2016. These include the Austrian aerospace company FACC, which lost EUR 42 million to this kind of fraud and subsequently replaced its CEO.[16] MELANI also knows of some cases in Switzerland. Whether in Switzerland or abroad, this type of fraud is not in decline, but rather appears to be honed even further. It follows the typical pattern of criminal groups active on the internet: proven methods are retained, with improvements and refinements of the individual steps of the method.

Social networks are a gold mine for obtaining initial information about the company. LinkedIn is especially interesting for scammers because profiles contain information on business relationships or the identity and function of employees. Commercial registers or even company websites may provide useful information too. If the requisite information is not available online, the scammers make contact by phone to obtain information. There have also been cases in which a fax with the official letterhead of a cantonal administration has been sent to get at the company's information. The desired data mainly includes the email addresses of employees in the accounting department whom the scammers have targeted to make the payments in the end. Using the information from these initial contacts, targeted emails are then sent containing information that is plausible for the company in question.

Scammers mainly use domain names similar to a company's to send out emails that may at first glance appear authentic. MELANI is aware of twenty Swiss domain names registered in June 2016 alone that imitated company addresses. Using email addresses from these domains, the scammers wanted to trick recipients into believing that the emails were from real

[16] http://www.reuters.com/article/us-facc-ceo-idUSKCN0YG0ZF (as at 31 August 2016).

companies. Scammers also like to send emails from addresses indicating a certain position or profession such as lawyer.com, president.com or consultant.com.

Recommendation:

It is virtually impossible to prevent fraudulent emails of this kind from being sent. The scammers conceal their identity and background and can change addresses at any time as needed. The most important recommendation for prevention is therefore to raise employees' awareness, especially in positions such as accounting and finance that are targeted for this type of fraud. The following basic rule should be observed: do not give out information to unusual or dubious contacts, and do not follow any instructions in such cases even if under pressure. We also recommend that all companies check what information about the company is available online. Finally, procedures should be defined that all employees have to follow at all times. We recommend requiring collective signatures for money transfers.

4.6 Crimeware

Crimeware is a form of malware further developed by cybercriminals which, in criminological terms, ranks as computer crime and legally comes under causing damage to data and fraudulent misuse of a data processing system. Most infections in the first half of 2016 were due to Downadup (also known as Conficker). This worm has been around for over eight years and is spread via a security vulnerability in Windows operating systems that was both discovered and eliminated in 2008. There were changes toward the top of the ranking in the first half of 2016, however: the share of spambots has now passed the share of e-banking Trojans. The lethic malware, in second place, spreads drug spam and advertising for bogus goods. Necurs, in third place, specialises in spreading the Locky encryption Trojan and the Dridex e-banking malware. It is striking that the Dyre e-banking malware has dropped out of the top ranks of the statistics. Arrests in connection with Dyre have heavily reduced this malware at least in the short term. Read more about this in chapter 5.5.3.

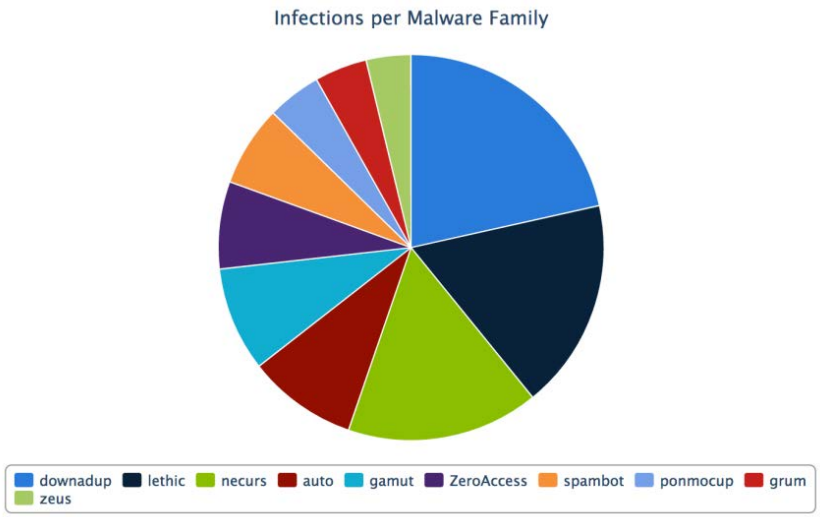


Figure 6: Breakdown of malware in Switzerland known to MELANI. The reference date is 30 June 2016. Current data can be found at: http://www.govcert.admin.ch/statistics/dronemap/

4.6.1 Increase in malicious Android apps in Switzerland

In the months of June and July 2016, thousands of text messages were sent to recipients in Switzerland purporting to be from Swiss Post, but containing a link to a website in Latvia. Upon clicking on the link, the victim was sent to a hacked website that tried to trick the victim into downloading a malicious Android app.[17] If the recipient ignored the displayed Android warning and installed the app, the device would be infected with malware.

Figure 7: Bogus SMS purporting to be from Swiss Post

The malware disguised itself with the name "*SwissPost*" and used the logo of Swiss Post. In the background, the app surreptitiously copied access data to popular apps such as Facebook, Uber and Viber, transmitting them to the hackers.

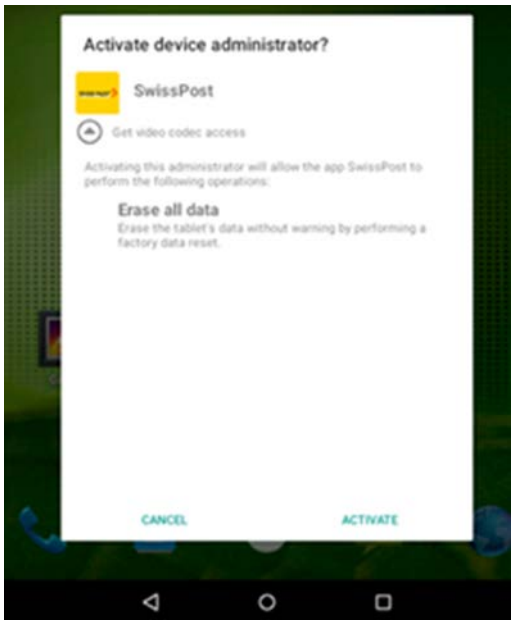


Figure 8: Malware disguises itself as Swiss Post app

Recommendation:

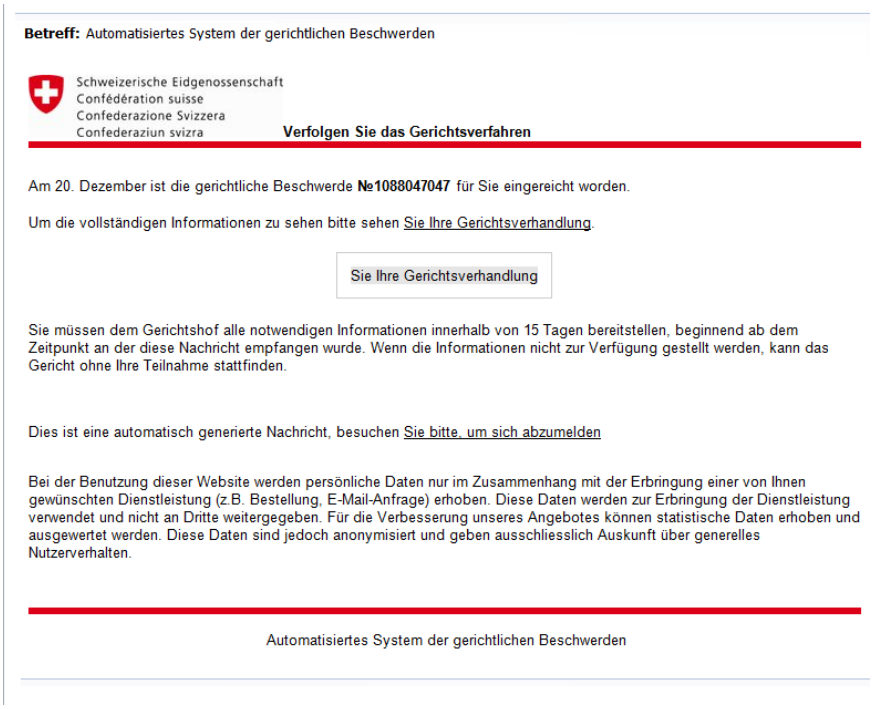
In general, no apps should be installed from third party sources. Instead, only the official app store of the manufacturer should be used.

[17] https://www.govcert.admin.ch/blog/24/sms-spam-run-targeting-android-users-in-switzerland (as at 31 August 2016).

4.6.2 Bogus summons leads to encryption Trojan

The threat posed by *encryption Trojans* rose further during the period under review. The simplicity of the approach and the fact that victims are still far too willing to pay ransoms have caused *ransomware* to spread even further.

To get users to click on an email link or open attachments and in that way to download ransomware to the computer, the attacker must be able to frame the context of the email in as plausible a way as possible. In many cases, the message purports to be from an institution that is known to the recipient and that the recipient believes to be credible. In that way, the recipient does not become suspicious. In its GovCERT blog in January 2016, MELANI drew attention to such an incident, concerning an email wave spread by the TorrentLocker ransomware.[18] The fraudulent email informed recipients that a lawsuit had been filed against them and that they were being summoned to court. To obtain additional information, the recipients had to click on a link and download documents. In that case, not only was the credibility of a public authority exploited, but also the uncertainty and fear of the users. Intimidation is a good way to trick victims into clicking on a link. For official summonses, courts never use email messages.



Betreff: Automatisiertes System der gerichtlichen Beschwerden

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Verfolgen Sie das Gerichtsverfahren

Am 20. Dezember ist die gerichtliche Beschwerde **№1088047047** für Sie eingereicht worden.

Um die vollständigen Informationen zu sehen bitte sehen Sie Ihre Gerichtsverhandlung.

Sie Ihre Gerichtsverhandlung

Sie müssen dem Gerichtshof alle notwendigen Informationen innerhalb von 15 Tagen bereitstellen, beginnend ab dem Zeitpunkt an der diese Nachricht empfangen wurde. Wenn die Informationen nicht zur Verfügung gestellt werden, kann das Gericht ohne Ihre Teilnahme stattfinden.

Dies ist eine automatisch generierte Nachricht, besuchen Sie bitte, um sich abzumelden

Bei der Benutzung dieser Website werden persönliche Daten nur im Zusammenhang mit der Erbringung einer von Ihnen gewünschten Dienstleistung (z.B. Bestellung, E-Mail-Anfrage) erhoben. Diese Daten werden zur Erbringung der Dienstleistung verwendet und nicht an Dritte weitergegeben. Für die Verbesserung unseres Angebotes können statistische Daten erhoben und ausgewertet werden. Diese Daten sind jedoch anonymisiert und geben ausschliesslich Auskunft über generelles Nutzerverhalten.

Automatisiertes System der gerichtlichen Beschwerden

Figure 9: Recipients were told that a lawsuit had been filed against them. To obtain additional information, the recipients had to click on a link and download documents. These documents contained malware.

4.6.3 Unsolicited job applications with ransomware

Other popular methods to trick recipients into clicking on a link or opening a file include appealing to the interests or needs of the victims or gaining their trust, such as by using their first and last names. Last May, emails circulating in Switzerland used exactly these methods. The victims were selected in a targeted manner and received emails containing unsolicited job applications. Recipients were asked to click on a link to receive access to the entire job

[18] https://www.govcert.admin.ch/blog/17/torrentlocker-ransomware-targeting-swiss-internet-users (as at 31 August 2016).

application file. The Dropbox link led directly to the Petya and Mischa encryption Trojans, however. The Locky malware, which is still very active both in Switzerland and abroad, has also been hiding recently behind supposedly harmless unsolicited job applications.

4.6.4 Encryption Trojans – technical aspects

In the first half of 2016, one of the technical improvements was discovered in version 3.1 of CryptXXX. This *virus* encrypts not only data on the victim's computer and also data on the storage devices attached to the computer. CryptXXX is also able to obtain passwords and other access data by downloading another *malware*, stiller.dll.[19]

CTB Locker, a ransomware that was very active especially in summer 2014, has resurfaced again. This is now a new version specialising in the encryption of website content. The method used to spread the virus is not entirely clear. Analyses of various sources indicate, however, that the attack is conducted via vulnerable WordPress sites. Once the website is infected, a message is displayed providing information on next steps to regain access to personal data. The malware randomly decrypts two files to show that the attackers are able to decipher the data. A mock customer service video is also shown, explaining how to obtain the *bitcoins* needed to pay the ransom. A chat function is also offered to contact the attackers if additional information is needed.[20] CTB Locker is not the only cryptotrojan that informs its victims of the infection in an imaginative way. The Cerber *macro malware*, which has surfaced also in Switzerland over the last six months, is the first cryptotrojan to make the ransom demand acoustically as well: "Attention! Attention! Attention! Your documents, photos, databases and other important files have been encrypted!" is announced from the computer loudspeaker.

To further increase psychological pressure on the victim, the Jigsaw blackmail Trojan uses a particularly insidious method: for every hour that passes, the ransomware deletes a certain number of documents, and at the same time it increases the ransom amount. Within 72 hours, all documents are deleted.[21]

Even Mac users can no longer imagine themselves safe. The KeRanger ransomware, which was discovered in March, is the first cryptotrojan able to attack OS X platforms.[22] With a valid certificate for Mac applications, criminals infected two installers of the version 2.90 of the BitTorrent program Transmission for OS X. The malware was available on the website between 4 and 5 March 2016. Anyone who downloaded Transmission for OS X during that time

---

19 https://www.proofpoint.com/us/threat-insight/post/cryptxxx-ransomware-learns-samba-other-new-tricks-with-version3100 (as at 31 August 2016). The CryptXXX cryptotrojan discovered for the first time in April is able to circumvent the decryptor tool developed by Kaspersky Lab.

20 http://www.bleepingcomputer.com/news/security/ctb-locker-for-websites-reinventing-an-old-ransomware/ http://www.heise.de/security/meldung/Admins-aufgepasst-Krypto-Trojaner-befaellt-hunderte-Webserver-3116470.html (as at 31 August 2016).

21 http://blog.trendmicro.com/trendlabs-security-intelligence/jigsaw-ransomware-plays-games-victims/ (as at 31 August 2016).

22 The FileCoder ransomware, which was discovered by Kaspersky Lab in 2014, was still incomplete at the time of its discovery and therefore could not damage OS X operating systems. http://researchcenter.paloaltonetworks.com/2016/03/new-os-x-ransomware-keranger-infected-transmission-bittorrent-client-installer/ (as at 31 August 2016).

was infected. The infected Transmission installation files were then deleted. Apple has now revoked the *certificate*.[23]

Recommendation:

According to Kaspersky Lab, the volume of ransomware quintupled between April 2015 and March 2016 compared with the same period of the previous year. This exponential increase entailed that over the past six months, organisations have published a higher number of warnings. In May, the German Federal Office of information Security (BSI) published a detailed report on ransomware; and in collaboration with Europol and two IT security firms (Kaspersky Lab and Intel Security), the Dutch police launched the no-moreransom.org website. In cooperation with several Swiss partners, MELANI organised a ransomware awareness day in May, drawing attention to four measures:

- Regularly make a backup of your data. The backup should be stored offline, i.e. on an external medium such as an external hard disk. Thus make sure that the medium where the backup is saved is disconnected from the computer after the back-up procedure is complete.
- Keep installed software and plug-ins up to date.
- MELANI recommends that internet users not open suspicious email attachments, even if they come from supposedly trustworthy senders.
- Additionally, users should install virus protection and keep it updated.

Measures against encryption Trojans:

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

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

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

No More Ransom project:

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

Rules of Conduct ➔ E-Mail

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

[23] http://www.welivesecurity.com/2016/03/07/new-mac-ransomware-appears-keranger-spread-via-transmission-app/ (as at 31 August 2016).

4.7 Preventive measures

4.7.1 First MELANI awareness day: Ransomwareday

Together with numerous partners, MELANI launched an awareness day for the first time on 19 May 2016. To raise public awareness for *ransomware*, organisations from a variety of sectors, software manufacturers, federal offices and numerous Swiss associations and consumer protection organisations took up the issue on that day and released various publications. It is still being clarified to what extent a day like this will be repeated.

5 Situation internationally

5.1 Espionage

5.1.1 Espionage attack interferes with election campaign

On the evening before the national convention of the Democratic Party of the United States in Philadelphia, Debbie Wasserman Schultz resigned as chairperson of the Democratic National Committee (DNC) – evidently unfortunate timing for a change in the party leadership.[24] What happened? Two days before, Wikileaks[25] published about 20,000 internal emails of the DNC leadership. The emails indicated that the DNC had not only preferred Hillary Clinton as the party's nominee, but also coordinated efforts to give her an advantage against her toughest rival, Bernie Sanders.

But the story began already more than a month before that, when the Washington Post[26] reported on a hacker attack against the DNC's digital infrastructure. Already for a whole year, the attackers combed through analyses on the Republican opponent Donald Trump and, as the Wikileaks publication impressively shows, they also read the DNC's email communications.

At the end of April 2016, DNC IT officers noticed strange occurrences and decided to consult experts from the Crowdstrike firm. The incident response team of Crowdstrike then discovered two independently operating attackers in the party's network, whom they identified as the known groups COZY BEAR and FANCY BEAR. FANCY BEAR – known for the 2015 attack on the German Parliament – had already operated in the DNC network since summer 2015, according to Crowdstrike. The presence of COZY BEAR was not shown until April 2016. In its report, Crowdstrike suspected two different Russian intelligence agencies to be behind the attacks.[27] On the same day, a supposedly Romanian hacker with the pseudonym Guccifer 2.0 claimed sole responsibility for the attack. He also announced that he would pub-

---

[24] https://www.washingtonpost.com/politics/hacked-emails-cast-doubt-on-hopes-for-party-unity-at-democratic-convention/2016/07/24/a446c260-51a9-11e6-b7de-dfe509430c39_story.html (as at 31 August 2016).

[25] https://wikileaks.org/dnc-emails/ (as at 31 August 2016).

[26] https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html (as at 31 August 2016).

[27] https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/ (as at 31 August 2016).

lish excerpts of his loot on Wikileaks. This prompted Crowdstrike to update its report and expose Guccifer 2.0. Crowdstrike later received support from the cybersecurity firms Fidelis Cybersecurity and Mandiant, which drew the same conclusions,[28] as well as Thomas Rid, professor in security studies at King's College London. He discovered an identical command & control (C&C) server in the DNC malware that had already been used in the attack on the German Parliament. The Romanian origins of Guccifer 2.0 and thus his credibility were called into question at the latest when he was unable to communicate fluently and comprehensibly with a journalist whose native language was Romanian.

Conclusion:

The incident shows impressively how power-political influence in cyberspace can be turned out to be. Public opinion can be influenced quickly by hacking sensitive data of a competitor and selectively publishing incriminating information.

5.2 Data leaks

5.2.1 Unwanted publication of electoral registers

Not once but twice, data leaks of electoral registers made the headlines in the first half of 2016. On 30 March 2016, an anonymous hacker published a file containing the personal information of 50 million Turkish citizens.[29] The information included names, addresses, first names of parents, places of birth, dates of birth, and national identification numbers. Accompanying the data, a statement was published accusing the Erdogan government of doing too little to protect citizens' data. It turned out that the information was not current but rather from the year 2008. The authenticity of the data was confirmed by the Associated Press news agency, however. When such data is published, there is always a danger that it might be used for identity theft.

Only one week later, an even more extensive data leak became public in the Philippines.[30] 55 million Filipino voters were published due to a hack of the database of the Philippine Commission on Elections (COMELEC[31]). According to Trend Micro, a security software provider, the data also included sensitive information such as passwords and 15.8 million registered fingerprints.[32] The actual incident took place already on 27 March 2016, when Anonymous Philippines defaced the COMELEC website. A Facebook user referred to as Lulzsec Pilipinas made the stolen data available online a few days later.

5.2.2 What users did not want to share with their professional network

In addition to the data that has to be provided to public authorities as described in chapter 5.2.1, many internet users voluntarily make large amounts of their data available to private

---

28 https://www.wired.com/2016/07/heres-know-russia-dnc-hack/ (as at 31 August 2016).

29 https://www.wired.com/2016/04/hack-brief-turkey-breach-spills-info-half-citizens/ (as at 31 August 2016).

30 http://www.theregister.co.uk/2016/04/07/philippine_voter_data_breach/ (as at 31 August 2016).

31 COMELEC is one of three Philippine government commissions. Its main responsibility is to enforce laws and regulations for conducting elections in the Philippines.

32 http://blog.trendmicro.com/trendlabs-security-intelligence/55m-registered-voters-risk-philippine-commission-elections-hacked/ (as at 31 August 2016).

companies. Of course, these private companies are likewise not immune to data leaks. The professional network LinkedIn was already attacked in 2014. At the time, 6.5 million encrypted passwords were placed online. In mid-May of this year, a hacker going by the name of "Pace" offered 117 million sets of account information, including email addresses and encrypted passwords for 5 bitcoins (at the time approx. CHF 2,000).[33] LinkedIn confirmed the accuracy of the data. Even though the data is already four years old, the sale still constitutes a danger, because many internet users tend to change their passwords only rarely or not at all, and they use the same password for other services as well.

Recommendation:

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

Checklist on IT security for SMEs

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

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

Rules of Conduct for passwords

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

5.2.3 Twitter access data on the black market

It is not always the fault of online providers when access data ends up in criminals' hands. In July, 32 million sets of Twitter access data including passwords were offered on the black market.[34] In this case, it was assumed that the passwords were copied and then transmitted to the attackers by way of malware that had infected the browsers of the end users. Copying and selling access data is usually a lucrative additional source of income for criminals. Malware that is actually designed for other tasks such as e-banking fraud or encryption usually includes a *keylogger* as an additional function.

5.3 Industrial control systems

5.3.1 Malware in a German nuclear power plant

In the isolated area of the Gundremmingen nuclear power plant in Germany, two different types of malware were discovered on 18 removable storage devices and one computer dur-

[33] http://motherboard.vice.com/read/another-day-another-hack-117-million-linkedin-emails-and-password (as at 31 August 2016).

[34] https://techcrunch.com/2016/06/08/twitter-hack/ (as at 31 August 2016).

ing work in preparation for an audit. According to the nuclear power plant, the affected system was part of a loading machine for fuel assemblies and was used only for visualisation. It therefore had no influence on process control. According to media reports, the *malware* used was Conficker, which has been known and widespread since 2008. Although Microsoft made a security update available shortly after the malware appeared, MELANI/GovCERT.ch statistics show that Conficker is still the most widespread malware in Switzerland. The second discovered Malware is said to have been Ramnit. Ramnit became active in 2010. The Ramnit botnet was deactivated in 2015 by Europol and the security firm Symantec.

It may at first seem astonishing that a *Windows vulnerability* was not patched at a nuclear power plant. But the affected system was in the isolated area of the facility, i.e. it was not connected to the internet. Moreover, industrial facilities are often certified upon installation. This means that the manufacturer guarantees flawless functioning in exactly that configuration. If the system is changed in any way – even through a security update – the guarantee is voided. Because systems are operated in isolation, the risk of a malfunction caused by an update is considerably greater than the threat emanating from a security vulnerability. Due to the complete isolation of the systems, internal security vulnerabilities should be irrelevant. But there are still ways in which malware can be introduced into areas protected in this way:

- Because there is no internet connection, the systems cannot be maintained and controlled online. A certain threat to the network arises here if external systems, such as laptops or *USB sticks* are connected with the network for the purpose of maintenance or import/export of data. In doing so, the *air gap* – or isolation of the system – may have been circumvented and the virus introduced into the system. A real example is the computer worm Stuxnet, which was smuggled into an Iranian uranium enrichment plant a few years ago.

- The worm may have been on the computer from the start, but it had not attracted attention until now. This might have been the case if the computer was connected to the internet during installation and was isolated only afterwards, or if the data carrier used to transfer installation files to the computer was already infected.

Conclusion:

Targeted attacks generally rely on malware programmed especially for that purpose. The circulation of such malware is limited so as to stay below the radar if possible. This means a targeted attack against the nuclear power plant can be largely ruled out in this case.

However, if the infection is "inadvertent", there is always the risk of collateral damage: the malware might trigger malfunctions in the system, leading for example to a spontaneous shutdown. The systems that control the sensitive areas of a nuclear power plant are analogue, though, so that an event such as in Gundremmingen would not have had an impact on critical processes.

5.3.2 Publication about a cyberattack on a water company

In its Data Breach Report of March 2016, the security firm Verizon published the results of a proactive assessment carried out at a drinking water supply company.[35] The company was

[35] http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf (as at 31 August 2016).

referred to as "Kemuri Water Company (KWC)", but Verizon did not publish more detailed information about the company. During this assessment, traces of a hacker attack on the company website were found. The web-based payment application was compromised using well-known vulnerabilities. On this front-end server, the access data for the back-end server (IBM AS/400) were also saved in plain text in a *.ini file* and could be accessed by the attacker. The back-end system, which was in frequent use at the turn of the century, was not only running the database for payment settlement, but also KWC's accounting, customer data management, and *ICS* system. The ICS controlled hundreds of programmable logic controllers (PLCs) controlling valves and sensors for the water supply. Because the system was connected directly to the internet, the stolen data could be used to access the PLCs directly and manipulate the addition of various chemicals in the public drinking water supply. The assessment showed that the management of KWC had been informed of inexplicable incidents involving valves and pipes over the past 60 days. These incidents had led to the uncontrolled admixture of chemicals into the drinking water treatment process. Thanks to the system-independent monitoring of water quality, manual intervention was able to prevent any threat to water users.

At the time, however, these incidents were not recognised as a cyberattack. The subsequent investigation concluded that the attackers did not have detailed information about the facility and thus were able to cause only limited damage. With more time and information, this attack could have been far more critical.

5.3.3 New type of malware with clear connection to ICS but unclear target

In June 2016, the security software provider FireEye published an investigation report on the *ICS malware* IronGate, which FireEye had discovered in the last half-year and which exhibits several remarkable characteristics.[36] For instance, it has the ability using *man-in-the-middle* to record information for five seconds that is being sent from the programmable logic controller (PLC) to the user interface. This information is subsequently replayed. While the operator sees the unalarming communication and fails to become suspicious, manipulated commands can be sent to the PLC in the background. For this purpose, the malware manipulates a *dynamic-link library (DLL)*, which serves as the intermediary between the PLC and the monitoring software. The malware also checks the running environment for the existence of sandboxes and analysis tools that are mainly used by security researchers and analysts. For instance, certain *droppers* of the *malware* do not work in a Cuckoo or VMware environment.

The malware targets the S7 PLCSIM software developed by Siemens and appears to be specifically geared toward a certain facility. FireEye suspects that the target is in the biogas industry. This can at least be suspected because of a found file labelled biogas.exe. Siemens ProductCERT confirmed that the malicious code does not work in a standard control environment. The malware is apparently designed to function in a simulator, which seems to indicate that the target is a research project or a test. But the malware also exhibits a very high level of quality and flexibility of development, so that this can be considered a next generation of Stuxnet. The author and purpose of this malware are still unknown. The malware was uploaded to VirusTotal in 2014, which confirms its existence since at least that time.

[36] https://www.fireeye.com/blog/threat-research/2016/06/irongate_ics_malware.html (as at 31 August 2016).

5.3.4 US government and car manufacturers agree on safety cooperation

Already in its last two semi-annual reports, MELANI discussed the security of means of transport and especially cars. At the beginning of the year, the US Department of Transportation signed a memorandum of understanding on safety with 18 major car makers. In particular, this was in the context of the increased use of IT in normal cars as well as developments relating to autonomous vehicles. In addition to general commitments to a forward-looking consideration of safety risks, mutual exchange of information, and cooperation to improve safety in road traffic, an explicitly included point refers to the improvement of cybersecurity in vehicles. The focus is primarily on the physical safety of persons, however; the security of systems is treated subsidiarily, as a possible cause of the danger to personal safety.

Conclusion:

More and more assistance services are being installed in cars and controlled by computer. The trust of users in the proper functioning of these systems is crucial. This is especially evident in the case of self-driving cars: to ensure that self-driving cars will be generally accepted in road traffic one day, all road users must gain a high basic level of trust in them first.

5.3.5 Car theft using electronics

Car manufacturers take personal safety very seriously (see chapter 5.3.4). Generally speaking, this area is already regulated. Manufacturers must expect claims for damages and may have to conduct massive recalls if they deliver faulty products that cause damage or endanger lives. On the other side, there are systems in and on the car that have nothing to do with driving as such: instead of traditional physical keys, for instance, remote keys are used, or doors can even already be opened using a smartphone *app*. Many new cars no longer even have keyholes anymore, but rather are opened and closed only electronically.

With this development, some car makers appear to be prioritising functionality or speed of market launch over security: initially, some remote locks were so simplistic that a car thief merely had to intercept and record the signal. Merely by playing the recorded signal, the attacker was able to open the car door. Once products came onto the market that automatically unlocked the car when the driver approached it, car thieves quickly found out that the presence of a key could be simulated using modified radio devices. An accomplice simply has to get close to the owner and wirelessly forward the "key's" transmission to the thief, who is already standing next to the car (relay station attack). What makes this even worse is that if these systems are used, the engine can often be started by pressing a button once the system recognises the key's radio signal inside the car. It is often impossible or difficult to reconstruct how a car has actually been stolen. Thefts are simply reported to the police and the insurance company. Manufacturers are not under great pressure to install highly secure locking systems in their products as long as insurers are willing to pay for the loss.

The computerisation of cars not only entails the risk that they will be hacked and stolen. Once smartphones become the interface between the driver and the vehicle, mischief can also be caused by infiltrating the phone or otherwise exploiting that interface: in the case of the electric car Nissan Leaf, for example, it was possible to use an app and the vehicle identification number – which can be read through the windshield – to access data and operate

the car's air conditioning. While this app did not permit access to the vehicle electronics, the activation of the air conditioner could slowly but surely drain the car's battery.

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).

Checklist with measures for the protection of industrial control systems

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

5.4 Attacks

5.4.1 Cyber bank robbers steal USD 81 million

According to the central bank of Bangladesh, hackers stole access data to their internal payment system.[37] Hackers broke into the systems of Bangladesh Bank and installed their software tools designed especially for those systems. The attackers manipulated the database, e.g. the interfaces to the SWIFT client software responsible for international payment transactions. Not only were bogus transactions triggered, but also the traces in the log files were wiped. For example, the systems were prevented from printing out transaction confirmations, so that the transactions would remain undiscovered for as long as possible. On 4 and 5 February 2016, criminals misused the system to create several dozen orders to the Federal Reserve Bank of New York for the purpose of transferring large amounts from the account of Bangladesh Bank to accounts in the Philippines and Sri Lanka. Four of these orders totalling USD 81 million were successfully transferred to the Philippines. In the fifth transaction amounting to an additional USD 20 million, the intermediary bank noticed a typographical error. The hackers had spelled the name of a non-governmental organisation in Sri Lanka wrong, which caused the intermediary bank to check with Bangladesh Bank. Bangladesh Bank then stopped the transaction. At the same time, the Federal Reserve Bank of New York noticed an unusually high number of payment orders to private recipients. The alerted Bangladesh Bank was also able to cancel these bogus transactions and thus prevent a loss of about USD 850 million. The four successful transactions were traded for gaming chips at casinos in the Philippines, where the trace of the money is lost, given the lower density of supervision in gambling than in the classical financial system.

With this largest case of cyber fraud at a single bank so far, the law enforcement authorities of Bangladesh accused SWIFT of negligence. In their view, SWIFT was responsible for

[37] http://www.reuters.com/article/us-usa-nyfed-bangladesh-malware-exclusiv-idUSKCN0XM0DR (as at 31 August 2016).

checking the bank's entire system landscape for vulnerabilities after the SWIFT system had been installed. SWIFT in turn immediately rejected all responsibility in connection with the attack. SWIFT claimed that like all other SWIFT clients, Bangladesh Bank was responsible for the security of its systems and environment with interfaces to the SWIFT system. This is reminiscent of the discussions after the first cases of fraud using malware in e-banking: to what extent is a bank responsible for a fraudulent payment, and to what extent has the client breached a duty of care if the client's computer is infected with malware? Banks have meanwhile responded by increasing the security of e-banking systems. SWIFT has also responded and is now more strict about demanding compliance with security requirements.[38]

On 12 May 2016, a further incident targeting a business bank in Vietnam was discovered. By misusing the SWIFT network, which administers standardised transactions, a fraudulent transaction in the amount of USD 1.13 million was apparently triggered. In a third case, an Ecuadorian bank was said to be affected.

The report of the security service provider Symantec[39] mentions that the malware used to wipe the traces (*wipe components*) was already used in Operation Blockbuster. Blockbuster was responsible for the attack against Sony in November 2014. Identical components were found in the Vietnam case and modified functions of these components in the Bangladesh case. It is unclear whether the same culprits are behind the attacks on the banking systems, or whether the same program code was sold or shared in the cyber underground.

Conclusion:

Attacks on e-banking clients have for years been part of the standard repertoire of cybercriminals. At the latest since the Carbanak malware was used to attack banking networks directly one and a half years ago, it has become clear that similarly great efforts are being made to commit electronic bank robberies as they are in the field of highly developed espionage, provided that the income prospects are good. A detailed assessment of this trend can be found in chapter 6.1.

5.4.2 Carbanak 2.0 and similar attacks

Two years ago, an attack referred to as "Carbanak" caused turmoil in the international financial industry. For the first time, cyber scammers targeted a bank directly, not just end clients. The tools used, the professionalism and the persistence were similar to attacks considered to be *advanced persistent threats (APTs)*. The criminals' logic is relatively simple: while the effort is greater, the proceeds are also many times higher. The group had been quiet for some time. But already in September 2015, there were signs of activity again.[40] In February 2016, the software company Kaspersky confirmed the return of Carbanak 2.0. In another article, a

38 http://www.theregister.co.uk/2016/06/03/swift_threatens_insecure_bank_suspensions/ (as at 31 August 2016).

39 http://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-financial-attacks (as at 31 August 2016).

40 https://www.csis.dk/en/csis/blog/4710/ (as at 31 August 2016).

research team of the cybersecurity firm Proofpoint claimed to have discovered preparations by the Carbanak gang to attack banks in Europe, the Middle East, and the United States.[41]

One characteristic of Carbanak 2.0 is that the group not only targets banks: its victims now also include the accounting departments of other companies. In one case, the attackers changed the ownership structure of a major company. A straw man was smuggled in as a shareholder of the company. It is unclear, however, what the attackers' intention was. The incident was discovered before any damage was done.[42]

Carbanak is only the first case in a series of similar incidents. Cybercriminals are learning fast, integrating new techniques into their operations, and increasingly attacking the banks directly. Two other groups called Metel and GCMAN, for instance, are using the same approach. The Metel group operates similarly to the Carbanak group. In the cases observed so far, criminals emptied the ATMs of several banks overnight in Russian cities. The other part of the criminal group manipulated the affected accounts so that their account balance appeared to be the same as before the money was withdrawn. GCMAN in turn carried out transactions in the amount of USD 200 once a minute using *e-currency services* such as Bitcoin, Perfect Money and Payza. What is special about GCMAN is that the attackers moved around the internet undetected for 18 months.

5.4.3 Ransomware in hospitals

The wave of ransomware observed since the beginning of the year has also targeted critical infrastructures. Hospitals have recently become a frequent target of extortioners. As digitalisation progresses, hospital IT has become increasingly crucial also to the treatment of patients. In the first half of 2016, several cases became known involving hospitals in Germany and the US in which large sums of money were extorted and also paid to regain access to the hospital's infrastructure. At the Kansas Heart Hospital, perpetrators did not release all data after an initial payment and demanded more ransom. Hospitals appear to be on their way to becoming the target category with the highest extortion sums. The perpetrators know that a hospital has to react quickly and regain access to its IT infrastructure in order to save lives. This is why the hospital sector has become a preferred target.

A further challenge is the fact that more and more diagnostic and analysis devices are computer operated. These devices are tested and certified for use in the medical field, the IT department of a hospital is usually not able to update the operating system or install an antivirus program, because doing so would change the device and lead to a loss of certification. IT departments of hospitals often also lack the resources or expertise to perform an update on such specialised systems.

In the past, it was possible to operate these systems offline. But now that the devices are being networked, more and more vulnerable systems whose security cannot be guaranteed are being connected to the IT network of hospitals. Given this, it is especially important to work together with device suppliers and to raise their awareness accordingly.

---

41 https://www.proofpoint.com/uk/threat-insight/post/carbanak-cybercrime-group-targets-executives-of-financial-organizations-in-middle-east (as at 31 August 2016).

42 https://securelist.com/blog/research/73638/apt-style-bank-robberies-increase-with-metel-gcman-and-carbanak-2-0-attacks/ (as at 31 August 2016).

Finally, digital patient data may also be of value to attackers. Personal medical files may become targets of espionage or sabotage. Mass data on treatments, their results and characteristics are very helpful for the further development of existing treatments and the search for new treatments using big data analysis. Such data is also a desirable target for individuals and companies with illegal intentions. The right questions must therefore be asked when digitising patient files, namely what the risks are and how they can be minimised, and a procedure must be defined in case the loss of data must be communicated to patients.

5.4.4 Japanese ATMs looted

Between 5am and 8am on Sunday, 15 May 2016, about 1,700 ATMs in Japan were looted in a large-scale and coordinated action, with losses equivalent to nearly CHF 17 million. In order to carry out nearly 14,000 withdrawals in such a short period of time, approximately 600 persons used up to 1,600 counterfeit credit cards. Data stolen from clients of South African Standard Bank was stored on the magnetic stripes of the counterfeit cards.

Foreign credit cards hardly used to be accepted at Japanese ATMs. Some time ago, the government called upon banks to change this policy so as to make it easier for foreign tourists to withdraw money. But many ATMs are apparently not set up to read the chip on the credit card. These machines therefore still access the magnetic stripe, which is easy to copy. The incidents also show that detection of fraudulent withdrawals using foreign credit cards still has to be improved.

One reason for the extraordinary amount of the damage is probably that the withdrawal limit at many ATMs at the time of the incident was JPY 100,000 or JPY 200,000 (corresponding to about CHF 900 and CHF 1800). As a reaction to the incident, the limits were reduced to at most JPY 50,000.

5.4.5 Anonymous & Co: #campaigns

The first half of 2016 was characterised by numerous, at times intense activities of hacktivists against organisations seen as centres of power.

Already at the beginning of the year, the Anonymous collective issued a "call to arms". The plan was another attack on the global financial system using the mythological name "Operation Icarus". "Like Icarus, the powers that be have flown too close to the sun and the time has come to set the wings of their empire ablaze..."[43] The operation had already been planned at the time of Occupy Wall Street in 2011, as an online counterpart to the protests on the ground.[44] On 4 May 2016, a "30-day campaign against central bank sites across the world" was announced in a YouTube video. The same day and with the help of the hacker group Ghost Squad, Anonymous flooded the website of the central bank of Greece with web queries, so that their servers could not be reached for several hours. During the entire month of May, the actions of the #OpIcarus campaign included taking down the websites of more than 30 central banks. The most famous victims were the Bank of England, the New York Stock

[43] https://opicarus.wordpress.com/ (as at 31 August 2016).

[44] http://www.ibtimes.co.uk/opicarus-anonymous-hacker-reveals-inspiration-behind-latest-operation-evolution-hacktivism-1561457 (as at 31 August 2016).

Exchange, and the Vatican Bank. The strength of the attacks was roughly 250 Gbps.[45] Anonymous published the complete list of the targets, which included more than 200 websites, and announced on Twitter that more was to come.

The hacker group Ghost Squad, which used to be a subgroup of Anonymous,[46] announced an analogous operation called "#OpSilence" for the month of June. The goal was to punish the media whose coverage of the war in Palestine or the actual crimes committed in Syria was biased or non-existent.[47] Ghost Squad did not keep to the announced dates, however, and launched the attack already on 31 May by taking down the email systems of the CNN and Fox News services for several hours.[48] For the entire month of June, it announced further attacks against media. Possible targets mentioned were NBC and MSN; the threats turned out to be empty, however. An interesting side story was that Ghost Squad emphasised the independent nature of its operations, claiming to have nothing (more) to do with Anonymous.

Conclusion:

The loose connection between Anonymous and similar groups such as Ghost Squad has resulted in a series of uncoordinated, more or less spectacular announcements and attacks. Because Anonymous has no membership structure and no official speakers or other persons responsible for the movement as a whole, in principle anyone can publish messages in the name of Anonymous and generate media interest in that way.

5.4.6 xDedic: buying access to hacked services in online shops

In June, Kaspersky published details on the investigation of an underground market named xDedic that it conducted together with a European internet service provider. Since 2014, access to about 70,000 hacked servers using *Remote Desktop Protocol* (for remote access to Windows servers) has been offered on xDedic – starting already at USD 6. Those servers are then used as a starting point for further attacks (*DDoS*, *spam*, etc.), or access directly targets the data and programs on a server. Servers with access to payment terminals are especially interesting. Shortly after the Kaspersky report was published, the site disappeared, but it later resurfaced on the *Tor network*.

---

45 http://thefreethoughtproject.com/anonymous-hits-york-stock-exchange-world-bank-vatican-total-corporate-media-blackout-ensues/ (as at 31 August 2016).

46 http://thefreethoughtproject.com/not-anonymous-hacking-group-declares-war-mainstream-takes-cnn-fox/ http://anonhq.com/anonymous-opsilence/ (as at 31 August 2016).

47 http://news.softpedia.com/news/anonymous-announces-opsilence-month-long-attacks-on-mainstream-media-504760.shtml (as at 31 August 2016).

48 http://thefreethoughtproject.com/not-anonymous-hacking-group-declares-war-mainstream-takes-cnn-fox/ (as at 31 August 2016).

Conclusion:

This case is representative of the increasing trend toward division of labour in the criminal cyber underground. Actors with less know-how can access a whole range of services to conduct attacks with minimal effort and expertise. After being revealed by Kaspersky, the site disappeared but later resurfaced on a platform with more anonymity for administrators, sellers and buyers. This shows that operators are able to adjust a profitable market to the circumstances in order to keep it running.

5.5 Preventive measures

Apart from raising awareness, the most effective preventive measure is the capture of cybercriminals. Many people believe that cybercrime arrests are difficult or even impossible. But several raids show that successes are possible in this area as well.

5.5.1 Raid on the darknet

During an international raid targeting operators and users of illegal web platforms, nine suspects were arrested. Additionally, 69 residences and companies in Germany, Switzerland, France, the Netherlands, Lithuania, and Russia were searched. Nine strong suspects were arrested. The investigations targeted various German-language forums of the underground economy. These were used to trade illegal goods such as weapons, narcotics, counterfeit money, counterfeit identity cards, and stolen credit card and online banking data. The criminal services included *DDoS* attacks or infections of computers with *malware*.

The alleged main operator of a total of three forums is a 27-year-old Bosnian citizen. The accused was arrested in Bosnia and Herzegovina on 24 February 2016 and is now in pretrial detention.

Extensive evidence was secured, especially numerous computers and storage devices, a firearm, narcotics, and assets in the amount of approximately EUR 150,000. Additionally, numerous servers in France, the Netherlands, Lithuania and Russia running criminal online marketplaces were confiscated. A notice that the server had been seized was displayed on the associated websites.[49]

49 https://www.bka.de/SharedDocs/Pressemitteilungen/DE/Presse_2016/pm160229_UndergroundEconomy.pdf?__blob=publicationFile&v=1 (as at 31 August 2016).

Figure 10: The police downloaded this banner onto the seized webservers.

Conclusion:

This action is further proof that there is no complete anonymity on the internet. It also underscores the importance of international cooperation in the fight against internet crime.

5.5.2 Angler and Nuclear exploit kit activity subsides

Probably the two most famous *exploit kits* vanished almost entirely in the first half of 2016. The reasons for their disappearance differ, however. In April 2016, the security firm Check Point unveiled an analysis with numerous details about Nuclear. This probably scared off the operators to the extent that they went underground and at least temporarily suspended their activity. Since 30 April, the French exploit kit experts Kafeine have not recorded any more attacks by Nuclear.[50]

According to Kafeine, the Angler exploit has disappeared completely since 7 June. Here again, the question arises regarding the trigger of this sudden disappearance. A possible explanation is the arrest by Russian authorities during this period of 50 alleged cybercriminals connected with the Lurk malware. The arrested persons are said to have stolen money from Russian bank accounts using a Trojan. The infection vector of these attacks is directly connected with the Angler exploit kit. It is an open question whether some of the authors of the Angler exploit kit were arrested in these raids, or whether they simply got cold feet for fear the arrested persons might snitch on other criminals. But unfortunately, anyone hoping that the use of exploit kits by criminals would decline after the disappearance of Angler would have been disappointed. The use of kits has merely shifted: after the end of Angler, the use of the Neutrino exploit kit increased strongly.

[50] http://www.securityweek.com/exploit-kit-activity-down-96-april (as at 31 August 2016).

5.5.3 Several arrests of Dyre instigators in several countries

In February, the Forbes news site reported that in November 2015, Russian authorities had disabled the *botnet* of the e-banking Trojan Dyre and arrested the leading members of the criminal organisation.[51] According to IBM, Dyre was the most active banking Trojan in the year 2015, responsible for about 25% of worldwide cases of banking fraud. It had also spread like wildfire in Switzerland. Initially, the Trojan mainly targeted SMEs. For instance, the scammers were able to steal a seven-digit figure from a business in the canton of Fribourg.[52] Later, Dyre also focused on private users. Although the raid – which probably had been ordered by a Russian governmental body – was not officially confirmed, the activities of Dyre came to a halt, as the malware statistics published by GovCERT.ch clearly show. Now, only the infections of systems remain that had never been cleaned. According to Forbes, however, this is not the end of the Dyre malware, since the *source code* is now freely available on the internet.

6 Trends and outlook

6.1 Highly developed attacks – criminals now also an APT

More and more frequently, criminals are investing greater effort to obtain higher gains. They are working in a more targeted way and trying to optimise effort and returns. Alongside the attacks on the interbank messaging system SWIFT at the beginning of this year (chapter 5.4.1) and the attacks attributed to Carbanak (chapter 5.4.2), attacks against end users also are developing rapidly. The division of labour and reuse of malware in the digital underground market are favouring this trend.

For a long time, the principle applied that as little effort as possible should be invested in scams. This meant that the worst-protected system was the most worthwhile target. These low-hanging fruit were mainly end users' computers employed to carry out e-banking and similar transactions. Just a few years ago, direct attacks on financial institutions were solely the domain of movies and television. The effort and the required professionalism were considered too high at the time. The trend toward spectacular cyber robberies is not very astonishing, however, and has several causes:

- Firstly, the software necessary for complex attacks of this kind is meanwhile available on the underground market. Criminals have now also acquired the necessary expertise. This circumstance is helped by the fact that the dividing line between state-sponsored and criminal attacks is becoming increasingly blurred.

- Another important reason is that money laundering has become more difficult. Fortunately, it has become a challenge to find people naive enough to be recruited as money mules. What makes things more difficult for criminals is that money mules are generally taken out of circulation after only a single attempt. Criminals therefore look for alternatives that do not rely on money mules or that use money mules efficiently.

---

51 http://www.forbes.com/sites/thomasbrewster/2016/02/08/russia-arrests-dyre-malware-masterminds/#5d5cf29a1e02 (as at 31 August 2016).

52 http://www.20min.ch/digital/news/story/E-Banking-Trojaner-zielt-auf-Schweizer-Firmen-ab-23497999 (as at 31 August 2016).

The simplest way to launder money more efficiently is to have each money mule transfer higher sums. Companies are now being targeted by criminals because larger transfer amounts are not as obvious there.

The incidents in chapters 5.4.1 and 5.4.2 are examples showing that new ways are sought and unfortunately also found to eliminate the traces of the money flow. The groups involved in the Carbanak and Metel malware manipulated ATMs in such a way that they spat out money at specific times. Because the withdrawals were made in cash, no money laundering was necessary. The GCMAN group used electronic currencies, where tracing the money flow is also more difficult. In the cyber robbery of the central bank of Bangladesh, the money from the four successful transactions was exchanged into gaming chips at casinos in the Philippines, where the trail of the money was lost. The regulatory density for gambling is lower than in the classical financial system. All in all, greater returns for criminals also make more elaborate and professional money laundering possible.

But anyone believing that professional attacks are displacing simple attacks would be mistaken. Experience shows that the old forms of attack do not die, but instead are passed on to a different set of perpetrators. *Phishing* attempts are still common. While these attacks are no longer as successful as they used to be, they still take place and have to be defended against. Not only is the pie being redistributed, but it is also growing overall.

6.2 The future of the internet – from a technological and social perspective

The first cars did not have a roof, let alone a safety belt or other precautions to protect the driver. In fact, most drivers were the only ones on the road, and they were happy that the vehicle moved in the desired direction at all. The situation was similar during the pioneering years of the internet. As the US computer engineer Danny Hillis already said in the 1980s, "There were only two other Dannys on the Internet then. I knew them both. We didn't all know each other, but we all kind of trusted each other."[53] Internet users were happy that the network worked at all. In road traffic, traffic rules were introduced over time and as the number of accidents grew, safe roads were built, and regulations were enacted requiring cars to be equipped with safety belts, crumple zones, ABS and airbags. On the internet, however, the original architecture was left more or less the same, and binding internet traffic rules did not exist. Security was left to users and services employing the internet. Staying within our analogy, car drivers simply had to wear a bigger helmet, but even that only voluntarily.

In physical terms, the internet consists of 60,000 individual networks, referred to as *autonomous systems (ASs)*. These autonomous systems are primarily offered by telecommunications providers, but also larger and smaller private and public organisations operate their own ASs. Within a single AS, the operator has control over the network, but beyond the boundaries of one's own AS, a common regulatory framework applies, namely the *Border Gateway Protocol (BGP)*. BGP was developed in the 1980s for the interplay of just a few individual networks and still governs which paths our data packets take through the global network. This makes the backbone prone to error and easy to influence. As the corpus of Snowden document shows, this has also been exploited.

[53] https://www.ted.com/talks/danny_hillis_the_internet_could_crash_we_need_a_plan_b/transcript (as at 31 August 2016).

An alternative would be to build a new internet from scratch. Attempts in this direction have already been made. For instance, the SCION project at the Swiss Federal Institute of Technology Zurich offers a streamlined architecture that would facilitate path control, error isolation, and trust-based end-to-end communication. But until such an approach establishes itself among the 60,000 AS operators, quite some time will likely pass. Instead of making the basic structure fit for the future, new applications continue to be tinkered with, offering new functionalities on the basis of this antiquated foundation. As an example, big data and blockchain applications are dominating the headlines. Whether all of this means that the core of today's internet will have to be refreshed after all, or whether a new structure will emerge in parallel, remains to be seen.

Anyone wanting to participate in the network must necessarily accept certain disadvantages. Keeping the inadequacies of the internet in mind, however, the end users' awareness is raised that they must themselves be responsible for protecting their privacy and security. Anonymisation tools such as the *Tor browser* are becoming increasingly popular, and end-to-end encryption has been establishing itself since Edward Snowden's disclosures. By including the Signal protocol[54] in the popular WhatsApp instant messaging service, specialised software that used to be difficult to use has become more and more suitable for the masses.

In the end, however, risk management is the responsibility of every individual, every organisation, every company. Questions such as the following are becoming increasingly important in this regard: how and where are my data stored, who can access them, how are they used, and who gains financial advantages from them? The internet is now permanently caught in the tension between innovation, privacy, data security, and ultimately legal certainty. Because of the unstoppable progress of innovation, users can never rely on answers that have already been provided. Everyone is always being confronted with new questions. Anonymity and privacy are becoming increasingly difficult to enforce. This development is impressively illustrated by the Russian "Find Face" service: using merely a portrait picture of a person, it is possible to find their account in the social network VK.com. For now, this app exists only in Russian, and it can only access VK.com. But it is merely a question of time before facial recognition becomes common worldwide as an app. A photo will be enough to identify a person and to find all the associated information on the internet. Anonymity in public will then be history. Progress on the internet will compete with the right to privacy in very sensitive ways.

Society must find answers for this, and maybe even define boundaries someday. The development of the internet, but also the development and transformation of social norms, has not been concluded by far. We are facing interesting phases of the development of the internet from a technological, social, but also from a legal and political perspective.

[54] Signal is a modern open source protocol with strong encryption, developed for asynchronous messaging systems.

7 Politics, research, policy

7.1 Switzerland: Parliamentary procedural requests

Item	Number	Title	Submitted by	Submission date	Council	Office	Deliberation status and link
Ip	16.3606	Who is responsible for cybersecurity in Switzerland?	Derder Fathi	17.06.2016	NC	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163606
Ip	16.3561	NATO declaration. Hacker attacks may trigger the mutual defence clause	Josef Dittli	17.06.2016	CS	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163561
Mo	16.3528	Responsibility for cyber defence	Ida Glanzmann-Hunkeler	16.06.2016	NC	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163528
Ip	16.3462	Ensure security of electronic patient data	Edith Graf-Litscher	15.06.2016	NC	FDHA	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163462
Ip	16.3413	Cyber risks and nuclear facilities	Bea Heim	09.06.2016	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163413
Ip	16.3394	Security cooperation with the Principality of Liechtenstein	Josef Dittli	07.06.2016	CS	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163394
Fr	16.1024	Interpol, cyber risks and cybercrime	Hansjörg Knecht	07.06.2016	NC	FDJP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20161024
Po	16.3382	Security in the internet of things. Promoting competence	Claude Béglé	06.06.2016	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163382
Fr	16.1022	Clearing up the cyberattack on Ruag	CVP Group	02.06.2016	NC	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20161022
Fr	16.1021	Cyberattack on Ruag and the DDPS. Draw the necessary conclusions!	Green Group	02.06.2016	NC	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20161021
Fr	16.1020	Control system and competence centre as groundbreaking tools in the fight against cyber risks	BDP Group	02.06.2016	NC	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20161020
Ip	16.3359	How does the federal government support the cantons in the prosecution of DDoS attacks (cyberattacks) when expertise is insufficient?	Marcel Dobler	31.05.2016	NC	FDJP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163359
Ip	16.3356	Finally redistribute funds and personnel for the cybersecurity fight	SP Group	31.05.2016	NC	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163356
Ip	16.3353	Purpose of the Swiss Security Network	Werner Salzmann	30.05.2016	NC	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163353
Po	16.3348	Creation of a Cyber Defence Council. Urgent for our sovereignty and security	Claude Béglé	27.04.2016	NC	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163348
Mo	16.3186	Cyber risks. Exchange of technical information	Corina Eichenberger	17.03.2016	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163186
Po	16.3058	Deactivation of analogue telephone lines. Impact on lift telephones and other alarm systems	Hans Egloff	08.03.2016	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163058
Ip	16.3440	What are the technological options for warning the entire Swiss population in the event of a disaster?	Mathias Reynard	15.06.2016	NC	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163440
Po	16.3381	Industry 4.0. Creation of a national coordination office	Claude Béglé	06.06.2016	NC	EAER	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163381
Ip	16.3337	Dynamic determination of the minimum bandwidth under the Telecommunications Services Ordinance	Martin Candinas	24.04.2016	NC	DETEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163337
Mo	16.3336	Increase of minimum	Martin Can-	27.04.2016	NC	DE-	https://www.parlament.ch/de/ratsbetrie

		internet speed as a basic utility to 10 megabits per second	dinas			TEC	b/suche-curia-vista/geschaeft?AffairId=20163336
Po	16.3313	Evaluate measures against rubberneckers that interfere with operations or violate personality rights	Bernhard Guhl	27.04.2016	NC	FDJP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163313
Ip	16.3296	Wi-Fi everywhere, except on Swiss trains?	Derder Fathi	26.04.2016	NC	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163296
Ip	16.3272	Fintech as a challenge for Switzerland	Elisabeth Schneider-Schneiter	26.04.2016	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163272
Po	16.3245	Evaluation of splitting up Swisscom into a public utility and a private services company	Balthasar Glättli	18.03.2016	NC	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163245
Po	16.3219	Roadmap for electronic voting	Marco Romano	18.03.2016	NC	FCh	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163219
Mo	16.3184	Digitalisation and computerised education. Joint further development of the digital education area	Jonas Fricker	17.03.2016	NC	EAER	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163184
Ip	16.3162	Revenge pornography	Yvonne Feri	17.03.2016	NC	FDJP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163184
Mo	16.3128	National Action Plan for reducing the digital divide	Jean Christophe Schwaab	16.03.2016	NC	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163128
Mo	16.3120	Save and strengthen SMEs. With the innovation coupon and other concrete instruments	Corrado Pardini	16.03.2016	NC	EAER	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163120
Po	16.3051	Deactivation of analogue telephone lines. Impact on lift telephones and other alarm systems	Joachim Eder	08.03.2016	CS	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163051
Mo	16.3007	Ensure modernisation of mobile networks as quickly as possible	Transport and Telecommunications Committee NC	01.02.2016	NC	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163007
Ip	16.3555	Autonomous driving, framework conditions and consequences	Susanne Leutenegger Oberholzer	17.06.2016	NC	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163555
Mo	16.3526	Stopping the deceptive practices aimed at Swiss consumers. No Swiss telephone numbers for feigning economic activities in Switzerland	Jean-François Steiert	16.06.2016	NC	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163526
Mo	16.3452	Roaming fees. Enough is enough	Elisabeth Schneider-Schneiter	15.06.2016	NC	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163452
Fr	16.5294	How does the Federal Council intend to strengthen management of "Digital Switzerland"?	Derder Fathi	08.01.1900	NC	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20165294
Ip	16.3387	Are digital invoices without a digital signature in compliance with the VAT?	Fabio Regazzi	07.06.2016	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163387
Mo	16.3310	Drones. Protecting the population from danger	Susanne Leutenegger Oberholzer	27.04.2016	NC	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163310
Po	16.3260	Introduction of a management instrument for digital questions	Claude Béglé	18.03.2016	NC	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163260
Fr	16.5056	Driving cars without a driver	Susanne Leutenegger Oberholzer	02.03.2016	NC	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20165056
Mo	16.3228	The Confederation should no longer have to be majority owner of	Ruedi Noser	18.03.2016	NC	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163228

		Swisscom					
Mo	16.3484	Establish the dominant position of Switzerland in blockchain technology	Claude Béglé	16.06.2016	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163484
	16.044	Preserving the value of Polycom. Total credit	Business of the Federal Council	25.05.2016	FC		https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20160044
Po	16.3256	Promotion of digitalisation in regulation (Regtech)	Martin Landolt	18.03.2016	NC	FDF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163256

7.2 EU: Directive on security of network and information systems (NIS Directive)

At the beginning of July 2016, the European Parliament agreed on the first European cybersecurity law. With the Directive on security of network and information systems (NIS), the EU aims to strengthen European resilience against cyberattacks. Companies operating essential services such as in the energy, transport, banking, and healthcare field, or providers of digital services such as search engines, online marketplaces, or *cloud services* must take adequate security measures to improve their resilience against cyberattacks. Serious hacker attacks on company computers must be notified. If this notification requirement is breached, penalties may be imposed. The European Parliament is convinced that by defining common cybersecurity standards and strengthening cooperation, enterprises will be supported in protecting themselves against the rising number of cyberattacks.

The NIS Directive has been in force since April 2016 and must now be transposed into national law by Member States within 21 months. They have an additional six months to define the "operators of essential services".

For Switzerland, adoption of the NIS Directive does not have any consequences for now. To what extent the NIS provisions and the requirements for participating in the digital single market may lead to Switzerland's autonomous implementation of proposals such as cybersecurity standards and the notification requirement remains to be seen. In the field of information assurance, Switzerland has so far successfully counted on voluntary cooperation of the State and the economy. It is in any event clear that adopting supplementary criminal provisions with a notification requirement in cyber cases necessitates the development and expansion of existing capacities and the creation of relevant monitoring bodies.

7.3 France: new rules for critical infrastructures

In France, ANSSI (Agence nationale de sécurité des systèmes d'information) published the first rules that legally require operators of critical infrastructures ("opérateurs d'importance vitale") to take protective measures against cyberattacks. The rules have been in force since 1 July 2016 and initially apply to companies in the healthcare, food and water sectors. Other sectors will follow. This legal basis was created in the context of the French military planning law of December 2013. It is now mandatory to take protective measures and report security incidents involving critical infrastructures. Sanctions are imposed for non-compliance with these rules.

France is the first country in Europe to adopt rules of this kind – even before the measures that will apply to all EU member states under the Directive on security of network and infor-

mation systems (NIS). But the NIS Directive will be broader, also covering companies not subject to the French rules.

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 SMS spam run targeting Android Users in Switzerland

13.07.2016 - MELANI / GovCERT.ch received several reports today about malicious SMS that have been sent to Swiss mobile numbers. The SMS is written in German and claims to come from the Swiss Post. But in fact, the SMS has been sent by hackers with the aim to infect Smartphones in Switzerland with a Trojan horse.

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

8.1.2 Dridex targeting Swiss Internet Users

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

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

8.1.3 Technical Report about the RUAG espionage case

23.05.2016 - After several months of Incident Response and Analysis in the RUAG cyber espionage case, we got the assignment from the Federal Council to write and publish a report about the findings. The following is a purely technical report, intending to inform the public about Indicators of Compromise (IOCs) and the Modus Operandi of the attacker group behind this case. We strongly believe in sharing information as one of the most powerful countermeasures against such threats; this is the main reason we publish this report not only within our constituency, but to the public as well.

➔ https://www.govcert.admin.ch/blog/22/technical-report-about-the-ruag-espionage-case

8.1.4 20min.ch Malvertising Incident

08.04.2016 - With this blog post we would like to share Indicators Of Compromise (IOCs) related to the attacks against 20min.ch, a popular newspaper website in Switzerland which got compromised and abused by hackers to infect visitors with an ebanking Trojan called Gozi ISFB. The IOCs shared in this blogpost may be used to spot infections within corporate networks.

➔ https://www.govcert.admin.ch/blog/21/20min.ch-malvertising-incident

8.1.5 Leaked Mail Accounts

18.03.2016 - MELANI/GovCERT has been informed about potentially leaked eMail Accounts that are in danger of being abused. MELANI/GovCERT provides a tool for checking whether your account might be affected: https://checktool.ch.

➔ https://www.govcert.admin.ch/blog/20/leaked-mail-accounts

8.1.6 Armada Collective is back, extorting Financial Institutions in Switzerland

11.03.2016 - A new wave of extortion emails has arrived in different Swiss Onlineshops. We have strong indications, that those extortioner are a copycat of Armada Collective.

➔ https://www.govcert.admin.ch/blog/19/armada-collective-is-back-extorting-financial-institutions-in-switzerland

8.1.7 Gozi ISFB - When A Bug Really Is A Feature

05.02.2016 - Gozi ISFB is an eBanking Trojan we already know for quite some time. Just recently, a new wave was launched against financial institutions in Switzerland. Similar to the attack we had already reported in September 2015, Cybercriminals once again compromised a major advertising network in Switzerland daily visited by a large number of Swiss internet users; they all become potential victims of the Gozi eBanking Trojan.

➔ https://www.govcert.admin.ch/blog/18/gozi-isfb-when-a-bug-really-is-a-feature

8.1.8 TorrentLocker Ransomware targeting Swiss Internet Users

21.01.2016 - On Wednesday, Jan 20 2016, we have noticed a major spam campaign hitting the Swiss cyberspace, distributing a ransomware called TorrentLocker. We have already warned about similar TorrentLocker attacks against Swiss internet users last year via Twitter. TorrentLocker is one of many ransomware families that encrypts any local file on a victim's computer and demands that the victim pays a ransom to have his files decrypted again. Since some ransomware families do not only encrypt files stored locally on the infected machine but also on any mapped network share, ransomware also represent a serious threat to corporate networks. To make sure that the malicious email goes through spam filters and gets opened by the recipient swiftly, the TorrentLocker gang is using a handful of tricks.

➔ https://www.govcert.admin.ch/blog/17/torrentlocker-ransomware-targeting-swiss-internet-users

8.2 MELANI Newsletter

8.2.1 Offline Zahlungs-Software im Visier von Hackern - Schweizer Unternehmen betroffen

25.07.2016 - In den letzten Tagen hat MELANI mehrere Fälle der Schadsoftware Dridex beobachtet, die sich gegen Offline Zahlungs-Softwarelösungen richtet. Solche Software wird in der Regel von Unternehmen verwendet, um eine grössere Anzahl an Zahlungen via Internet an eine oder mehrere Banken zu übermitteln. Werden Computer, welche solche Software verwenden, kompromittiert, sind die potenziellen Schäden entsprechend hoch. MELANI

empfiehlt Unternehmen deshalb dringend, Computer, welche für den Zahlungsverkehr verwendet werden, entsprechend zu schützen.

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

8.2.2 Vermehrt schädliche Office Dokumente im Umlauf

08.07.2016 - In den vergangenen Wochen ist eine Vielzahl von Meldungen bei der Melde- und Analysestelle Informationssicherung MELANI über schädliche Microsoft Office Dokumente eingegangen, welche via Email verbreitet werden und das Ziel haben, den Computer des Opfers mit Schadsoftware (Malware) zu infizieren. MELANI warnt deshalb explizit vor dem Öffnen solcher Office Dokumente und empfiehlt Internet-Benutzern erhöhte Wachsamkeit im Umgang mit Office Dokumenten sowie keine Office Makros auszuführen.

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

8.2.3 Technical Report about the Malware used in the Cyberespionage against RUAG

23.05.16 - The Reporting and Analysis Center for Information Assurance (MELANI) was tasked by the Federal Council to produce a report about the technical findings concerning the RUAG Incident. It is targeted towards network security professionals and is meant to support those responsible for security identifying risks within their own networks, as well as implementing additional security measures.

➔https://www.melani.admin.ch/melani/en/home/dokumentation/newsletter/technical_report_apt_case_ruag.html

8.2.4 Swiss Ransomware Awareness Day

19.05.16 - Together with partners, the Reporting and Analysis Centre for Information Assurance MELANI is organising an awareness day for ransomware today. The participants include organisations from various sectors, software manufacturers, federal offices and a range of Swiss associations and consumer protection organisations.

➔https://www.melani.admin.ch/melani/en/home/dokumentation/newsletter/ransomwareday.html

8.2.5 Handling security bugs, vulnerable infrastructure and a range of DDoS attacks: 22nd MELANI semi-annual report

28.04.2016 - In the second half of 2015, there were once again some spectacular cyber-related incidents worldwide. These were primarily DDoS attacks, phishing attacks and attacks on industrial control systems. Published today, the 22nd MELANI semi-annual report features handling security vulnerabilities as its key topic.

➔ https://www.melani.admin.ch/melani/en/home/dokumentation/newsletter/semi-annual_report-2-2015.html

8.2.6 Passwörter von 6‘000 E-Mail-Konten im Umlauf

18.03.2016 - Die Melde- und Analysestelle Informationssicherung hat 6‘000 Adressen zu E-Mail Konten erhalten, die offenbar gehackt wurden und nun möglicherweise für illegale Zwecke missbraucht werden.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/passwoerter-von-6000-e-mail-konten-im-umlauf.html

8.2.7 Betrügerische Telefonanrufe gegen KMUs im Zusammenhang mit dem eBanking Trojaner „Retefe“

16.02.2016 - Seit Anfang Februar 2016 erreichen die Melde- und Analysestelle Informationssicherung MELANI sowie die Koordinationsstelle zur Bekämpfung der Internetkriminalität KOBIK vermehrt Meldungen aus der Bevölkerung betreffend betrügerischen Telefonanrufen, welche das Ziel haben, eBanking Betrug zu ermöglichen.

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

8.3 Checklists and instructions

In the first half of 2016 MELANI didn’t publish any checklists and instructions..

9 Glossary

Term	Definition
.ini file	An initialisation file (INI file) is a text file containing key/value pairs. Initialisation files are often used as configuration files by Microsoft Windows applications.
Active Directory	Active Directory (AD) is a directory service that Microsoft developed for Windows domain networks. Starting with Windows Server 2008, however, Active Directory became an umbrella title for a broad range of directory-based identity-related services.
Advanced persistent threats (APTs)	This threat results in very high damages with an impact on an individual organisation or a country. Attackers are willing to invest a great amount of time, money and knowledge in the attack and generally have considerable resources at their disposal.
Air gap	In IT, air gap refers to a process that separates two IT systems from each other physically and logically, but nevertheless permits transmission of user data.
App	"App" (an abbreviation of "application") generally refers to any type of application programme. In common par-

	lance, the term now generally refers to applications for modern smartphones and tablet computers.
Autonomous system (AS)	An autonomous system (AS) is a collection of IP networks that are managed as a unit and are connected with each other via one or several shared interior gateway protocols (IGPs).
Batch job	Batch job is a term from data processing and refers to the method of operation of computer programs that completely, automatically and usually sequentially process the volume of tasks or data.
Binary file	A binary file is a file that, unlike a pure text file, also contains non-alphanumerical characters. It may thus contain any byte value. Files in binary format tend to be used to store data.
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 (BGP)	Border Gateway Protocol is the routing protocol used on the internet. It connects up autonomous systems.
Botnet	A collection of computers infected by malware. These computers can be controlled remotely and completely by an attacker (the botnet owner). Depending on the size, a botnet may consist of several hundred to several million compromised computers.
Browser	Computer programmes mainly used to display Web content. The best-known browsers are Internet Explorer, Opera, Firefox und 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.
Cloud Computing	Cloud computing (synonym: cloud IT) is a term used in information technology (IT). The IT landscape is no longer operated/provided by the provider himself, but rather obtained via one or more providers. The applications and data are no longer located on a local computer or corporate computing centres, but rather in a cloud. These remote systems are accessed via a network.
Command & control server	Most bots can be monitored by a botmaster and receive commands via a communication channel. This channel is called command & control server.

DDoS attacks	Distributed denial of service attacks. A DoS attack where the victim is simultaneously attacked by many different systems.
Digital certificate	Verifies the affiliation of a public key to a topic (person or computer).
Drive by infection	Infection of a computer with malware simply by visiting a website. Often the websites concerned contain reputable offerings and have already been compromised beforehand for the purposes of spreading the malware. The infection occurs mostly by trying out exploits for vulnerabilities not yet patched by the visitor.
Dropper	A dropper is an independently executable program file, generally serving to release a computer virus for the first time.
Dynamic-link library	Dynamic-link library (DLL) refers in general to a dynamic program library.
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.
Exploit	A loophole or bug in hardware or software through which attackers can access a system.
Exploit-Kit	Toolkits with which criminals can generate programs, script or lines of code to exploit vulnerabilities in computer systems.
Grey hat	Grey hats may break laws or restrictive interpretations of hacker ethics, but with the purpose of achieving an ethical objective.
JavaScript	An object-based scripting language for developing applications. JavaScripts are programme components integrated in HTML code enabling specific functions in internet browsers. For example, while checking user input on an internet form, a JavaScript can verify that all the characters entered of a telephone number are actually numbers. As is the case with ActiveX Controls, JavaScripts are run on the client's computer. Unfortunately dangerous functions can also be programmed with Javascripts. In contrast to ActiveX, JavaScript is supported by all browsers.
Keylogger	Devices or programmes in operation between the computer and the keyboard to record keystrokes.

MAC-Adresse	Media Access Control Unique and globally identifiable hardware address of a network adapter. The MAC address is written in the ROM of the adapter by the respective manufacturer (e.g. 00:0d:93:ff:fe:a1:96:72).
Macro malware	Malware installed with a macro. A macro is a sequence of instructions that can be executed with a simple call.
Malicious Code	Generic term for software which carries out harmful functions on a computer. This comprises amongst others viruses, worms, Trojan horses.
Man-in-the-middle	A man-in-the-middle attack (MITM attack) is a form of attack used in computer networks. The attacker stands either physically – or today usually logically – between the two communication partners, and has full control of data traffic between two or more network participants, using the attacker's system.
Phishing	Fraudsters phish in order to gain confidential data from unsuspecting Internet users. This may, for example, be account information from online auctioneers (e.g. eBay) or access data for Internet banking. The fraudsters take advantage of their victim's good faith and helpfulness by sending them e-mails with false sender addresses.
Pipe	A pipe or pipeline is a dataflow between two processes. Data read in first is also outputted first (first in, first out).
Point-of-Sale Terminals (POS)	Terminals in businesses where cashless payments with debit and credit cards are possible.
Programmable logic controller (PLC)	A programmable logic controller (PLC) is a digitally programmed device used to control or regulate a machine or facility. For some years, it has replaced hardwired control elements in most domains.
Ransomware	A form of malware used to extort money from the owners of infected computers. Typically, the perpetrator encrypts or deletes data on an infected computer and provides the code needed to recuperate the data only after a ransom has been paid.
Remote Desktop Protocol	The Remote Desktop Protocol (RDP) is a proprietary network protocol by Microsoft for displaying and controlling the screen contents (desktop) of remote computers.
Remote monitoring & control (M&C)	Remote monitoring & control (M&C) systems consist of one or more devices that control, regulate, and/or monitor the behaviour of other devices. In industrial production, the term "industrial control system (ICS)" is used.
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, for instance, in home networks, establishing the connection between the internal network and the Internet.
SCADA systems	Supervisory Control And Data Acquisition Systems. Are used for monitoring and controlling technical processes (e.g. in energy and water supply).
Security holes	Source Code Computer program written in a human-readable programming language.
Spam	Spam refers to unsolicited and automatically sent mass advertising, into which category spam e-mails also fall. The person responsible for these messages is known as a spammer, whereas the actual sending itself is known as spamming.
SSID	Service set identifier. Identifies the network name of the WLAN. All access points and terminal devices of the WLAN must use the same SSID to communicate with each other.
SWF animation file	The abbreviation SWF stands for Shockwave Flash. The manufacturer at the time, Macromedia, marketed Flash using the name Shockwave. Flash is the name of a platform for programming and displaying multimedia and interactive content.
Tor network	Tor is a network for anonymising connection data.
Trojan horses	Trojan horses (often referred to as Trojans) are programs that covertly perform harmful actions while disguised as a useful application or file.
USB	Universal Serial Bus Serial bus (with a corresponding interface) which enables peripheral devices such as a keyboard, a mouse, an external data carrier, a printer, etc. to be connected. The computer does not have to be switched off when a USB device is unplugged or plugged in. New devices are for the most part automatically identified and configured (depending on the operating system).
User interface	The user interface is the place or action with which a human enters into contact with a machine.
Virus	A self-replicating computer program with harmful functions that attaches itself to a host program or host file in order to spread.

Wipe	Wipe is an eraser software application used for securely deleting files. If a file is deleted by wiping, the program overwrites the data numerous times with zeros, special bit patterns and/or random data.
WLAN	WLAN stands for Wireless Local Area Network.
WPA2	Wi-Fi Protected Access 2. New security standard for Wireless-LANs in accordance with IEEE 802.11i specification. Successor to the WPA technique and to the WEP technique considered to be insecure.