Cyber Security 2018:

Artificial intelligence, malware & cryptocurrencies

Author: Swisscom Security
This report was prepared by Swisscom Security in close cooperation with other operational units.

May 2018

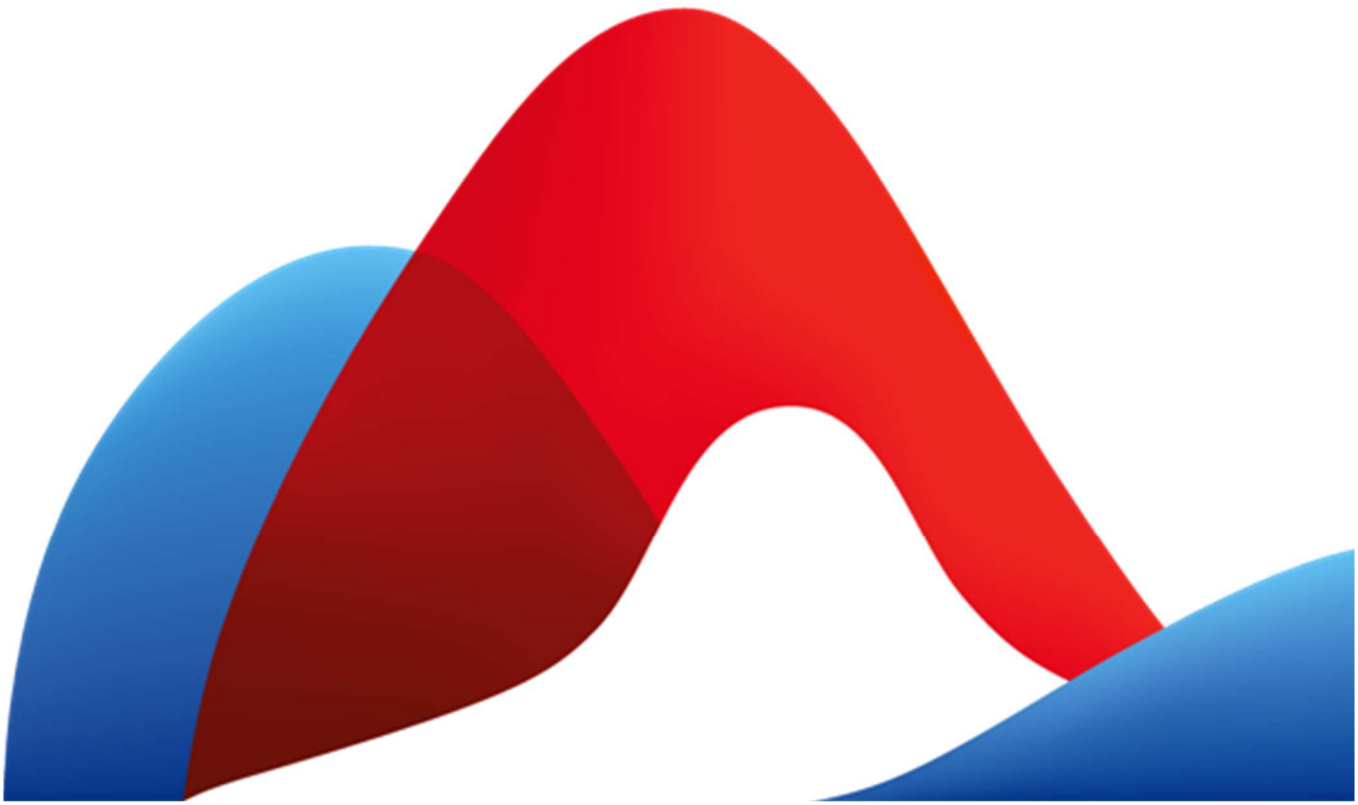

Table of contents

1. Introduction

2018 marks the second edition of Swisscom's annual Cyber Security Report. In addition to the threat situation, we look at two topics that are currently of concern to the security community within Swisscom, to our partners and customers and also at the international level.

The first is the use of artificial intelligence in the security environment. Here, we not only see AI being misused to carry out smarter attacks, but also its meaningful implementation as a way of identifying and responding to attacks and vulnerabilities more quickly and with greater accuracy.

The second topic concerns malware identified in our network. The spread of malware is and remains the most important tool for attackers in their attempts to compromise services, steal data and misuse systems that do not belong to them. Incidentally, most attacks are financially motivated, so it comes as no surprise that cryptocurrencies are also mentioned in our report.

This report is a joint effort of several departments within Swisscom.

For any readers in a hurry, we have provided a summary at the end of each main section with the key takeaways. Consequently, we did not include an overall summary at the end of this year's report.

In February, Swisscom disclosed that unknown parties had gained unauthorised access to its customer data via a sales partner in autumn 2017. The incident is not included in this report. The report aims to show general trends in Swiss cyberspace and does not discuss specific incidents. We have strengthened our internal security measures to ensure a similar incident does not occur again.

2. Status report – threat radar

Threats are born of the constant development of new technologies and their application and distribution across society. Potential threats must be identified at an early stage and systematically documented. We have chosen to depict the current threat status and its evolution using a radar image (Figure 1).

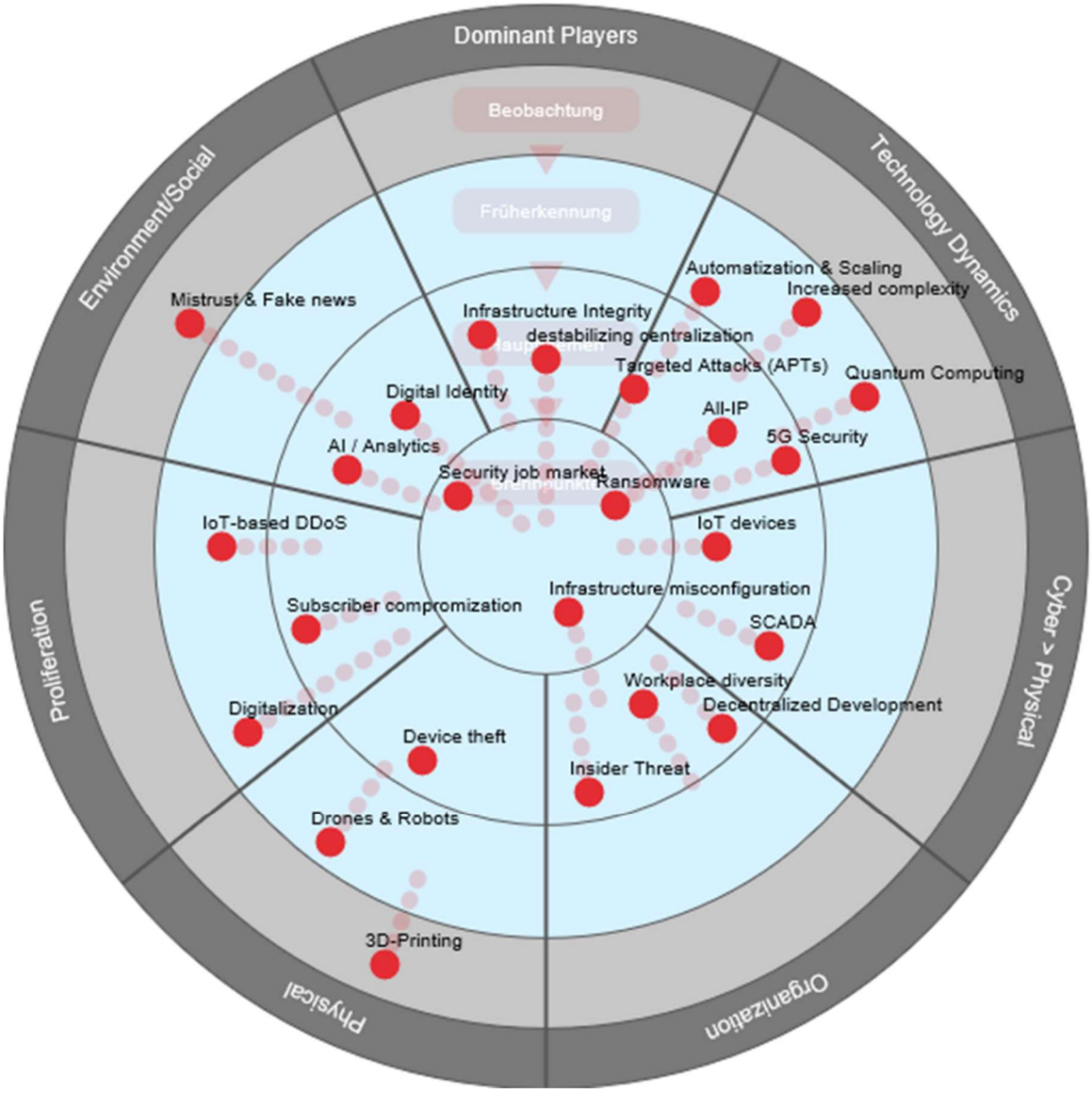

Figure 1: Threat radar

2.1 Methodology

The threat radar is broken down into seven segments that demarcate the different threat domains. The threats belonging to each of these segments can be assigned to one of four concentric rings. These circles indicate a threat's urgency and thus also the vagueness inherent in assessing such threats. The closer the threat is to the centre of the circle, the more concrete it is and the more important it is to take appropriate countermeasures. We refer to the rings as:

- **hot spots** in the case of threats that are already a reality and are being managed with a relatively large deployment of resources.
- **main topics** in the case of threats that have already materialised on occasion and can be managed with a normal deployment of resources. Often, defined processes already exist to efficiently counter threats of this nature.
- **early recognition** for threats that have not yet materialised or whose impact is currently very minor. Projects have been launched with the goal of addressing the growing significance of these threats at an early stage.
- **observation** for threats that will only arise in a few years. No concrete measures have been defined for handling these threats.

Moreover, the individual threats indicated by the points mentioned display a trend which may be increasing, decreasing or stable criticality. The length of the trend beam indicates how swiftly the threat's criticality is expected to change.

2.2 Threats

2.2.1 Dominant players

Threats arising through dependencies on dominant manufacturers, services or protocols.

Main topics	**Infrastructure integrity:** Key components of critical infrastructures may have vulnerabilities incorporated into them, either through negligence or deliberately, that endanger the security of the system. **Destabilising centralisation:** Strong centralisation in the structure of the Internet leads to cluster risks. The outage of one service, such as Amazon Web Services (AWS), can have a global impact.

2.2.2 Technology dynamics

Threats arising from the swift pace of technological innovation, which itself creates new threats as well as offering attackers new potential for launching attacks.

Urgent issues	**Ransomware:** Large amounts of critical data are encrypted and only (possibly) decrypted in exchange for the payment of a ransom.
Main topics	**Targeted attacks (APTs):** Key individuals are identified and attacked in a targeted manner to obtain relevant information or maximise the amount of damage inflicted. **All-IP:** The rollout of universal All-IP also increases the risks associated with VoIP technology. **5G security:** 5G is still a young mobile communications technology and its launch will not only offer us many new opportunities, but will also open the door to unknown threats.

Early recognition	**Automation & scaling:** Greater automation of technical operations will mean that the repercussions of successful attacks and misconfigurations will be greater. **Increased complexity:** The complexity of systems, especially across technology and corporate borders, is on the rise. This increases risk exposure and makes troubleshooting more difficult. **Quantum computing:** Quantum computers can make existing cryptographic methods useless because they can crack them in no time.

2.2.3 Cyber goes physical

Attacks through the cyberspace infrastructure will increasingly cause damage in the physical world.

Main topics	**IoT devices:** Devices with weak protection could be compromised and sabotaged. Such acts could limit the devices' integral functions, such as availability or data integrity. **SCADA:** Many control systems for critical infrastructure installations still exist which are protected poorly or not at all.

2.2.4 Organisation

Threats that arise through changes in the organisation or exploit weaknesses in the organisation.

Urgent issue	**Infrastructure misconfiguration:** Exploitation of misconfigured infrastructure components and/or vulnerabilities that are identified and rectified at a late stage.
Main topics	**Workplace diversity:** Apart from the many opportunities associated with the new working models, the uncontrolled use of such models, like "Bring your own Device" (BYOD) or the increased use of remote workplaces, exposes companies to greater risks. **Insider threats:** Partners or employees manipulate, misuse or sell information, whether through negligence or intentionally. **Decentralised development:** Traditional R&D departments are dying out, application development is moving closer to the business units and, at the same time, the release cycles are getting shorter.

2.2.5 Physical

Threats that arise from the physical environment that are generally more focused on physical targets.

Main topics	**Device theft:** The theft of devices, especially critical infrastructure components and increasingly IoT devices, may result in a loss of data or impair service availability.
Early recognition	**Drones and robots:** Clarification and attacks across long distances will become easier and cheaper.
Observation	**3D printing:** Improvements in the quality of 3D printers will make it cheaper and easier to produce e.g. keys and other physical devices.

2.2.6 Proliferation

Threats that are exacerbated by simpler, cheaper accessibility to IT media and expertise, because this opens up new potential areas of attack and also increases the availability of tools that can be used for attacks.

Main topics	**Subscriber compromisation:** Malware attacks mobile users' private data or is used to attack telecommunication and IT infrastructures.
Early recognition	**IoT-based DDoS:** Strong growth in the number of IoT devices coupled with low-level protection creates more "takeover candidates" for botnets. **Digitisation:** Increasing levels of networking between the real and virtual world and between individuals' private and work lives open up more avenues of attack.

2.2.7 Environmental/social

Threats arising as a result of socio-political changes or which are facilitated or become more valuable to attackers as a result of such changes.

Urgent issue	**Security job market:** Difficulties meeting demand for security professionals mean that less expertise is being deployed against attacks that are becoming increasingly complex and intelligent.
Main topics	**AI/analytics:** More data and better analytical models provided by AI can be misused to influence people's behaviour. Decisions are increasingly left up to autonomous systems. **Digital identity:** Authenticated, personal digital identities can be abused or stolen, e.g. to conclude contracts under other names.
Observation	**Mistrust & fake news:** Dwindling trust in governmental and social agencies can lead to a reduction in the exchange of information needed to identify and fend off potential attacks.

2.3 Conclusion

Our examination of the situation reveals that the complexity of the threat landscape is growing. Attackers are profiting from the increasing value of virtual assets, which also boosts their motivation to launch an intelligent, targeted attack. Furthermore, technological innovations and the convergence of the physical and virtual worlds are creating new opportunities for attack. Social changes are impacting our trust in one another and the way we work together. Attackers can exploit that to serve their own purposes.

Compared to last year, we can see that most of the known threats have remained relevant. Individual threats, such as **destabilising centralisation, 5G security, insider threats** and the use of **ransomware**, have become more critical since 2017. This may be attributable to the increased spread of new technologies (such as in the case of 5G security) or the further dissemination of tools to carry out attacks (as with ransomware).
We have corrected our initial assumption that threats across SCADA systems remain the same and now show the trend as an increasing one. For the future, we foresee an intensification of the problem as an increasing number of physical systems are linked more integrally to the Internet.
We consider the other threats to be less critical. In reality, we are not seeing 3D printing and IoT-based DDoS attacks as often as feared; however, they continue to be relevant.

We have also included new threats in our status report, which we already knew about last year but, unlike the other threats, we considered to be less critical. We have reassessed this appraisal. New on the radar are: **automation & scaling, increased complexity, quantum computing, decentralised development, AI/analytics** and **digital identity**. The technological momentum currently being seen in the area of artificial intelligence is striking. AI is not only having a positive impact on cyber security, but is also impacting the threat situation itself, e.g. by furnishing potential attackers with smart tools.

3. Artificial intelligence & cyber security

Artificial intelligence (AI), machine learning (ML) and deep learning are three related models, which we differentiate as follows:

Artificial intelligence	Artificial Intelligence (AI) is the intelligence displayed by machines through the use of logic, clear rules and decision trees.
Machine learning	Machine learning (ML) is a subcategory of AI that uses complex statistical techniques to enable machines to perform tasks with growing proficiency based on experience.
Deep learning	Deep learning is a subcategory of ML that allows software to train itself to perform tasks such as speech and image recognition by feeding huge amounts of data into a multiple neural network.

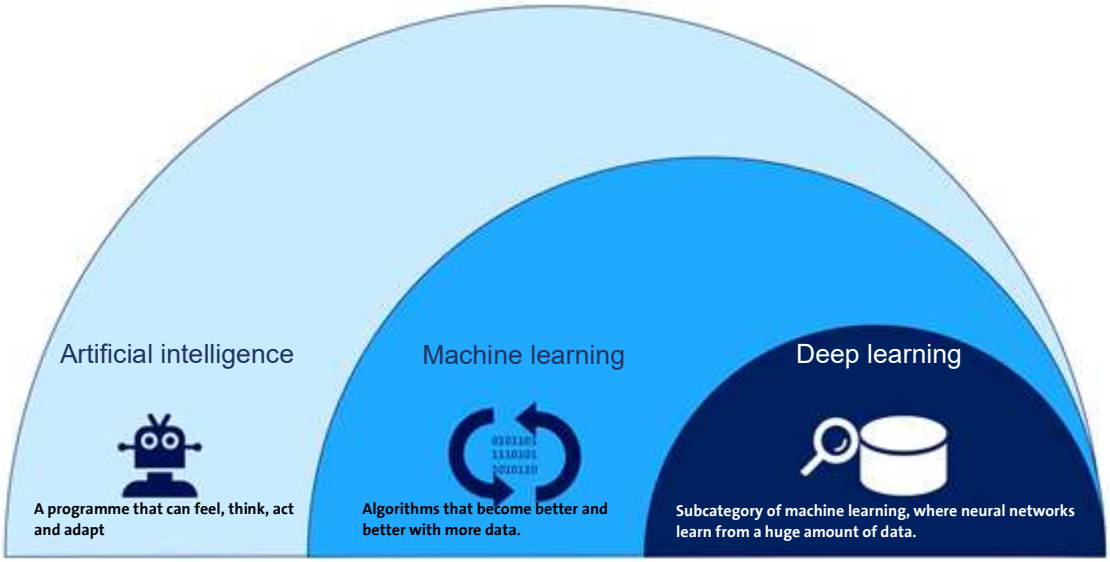

Figure 2: Artificial intelligence, machine learning and deep learning

3.1 Interview with Laure Willemin, Head of AI, Swisscom

Laure Willemin and her team develop and operate robust, scalable software systems using the latest AI, ML and deep learning technologies, including sentiment analysis, key phrase extraction and named entity recognition enablers. Laure loves tackling tough technological challenges and has been mastering them for over 15 years as a software developer, systems engineer and systems architect.

Laure, is artificial intelligence just an opportunity for Swisscom and our society, or should it also be classified as a security threat?

We do not see AI as a threat. The new technology can help us better understand large amounts of data and support the security efforts of our company. New technologies

often lead to uncertainty and misunderstandings and they can also be misused. But the positive effects far outweigh these concerns.

What are the most common misconceptions you have encountered so far about artificial intelligence and machine learning?

Primarily I'd say excessively high expectations regarding AI's potential. The most critical part of an effective system is the data. These data are often unstructured and the systems that process them need to be trained before they can be put to meaningful use. We can use the latest technology to do a good job of creating data models and are also seeing progress in work with smaller amounts of data. High data quality is still the most important component of successful AI applications, however.

Do you consider AI & ML to be disruptive factors in the Swiss industrial landscape? What do you think are the biggest changes that lie ahead?

AI is not a disruptive factor, but rather an essential element that will help us remain competitive in the future. With AI, Swiss industry will be able to automate repetitive processes and tasks and deploy qualified personnel for more complex, more creative work. At the same time, AI will help people make better decisions faster, such as in the real-time analysis of data.

How do you think AI, ML and deep learning can contribute to cyber security development?

Cutting-edge AI technology can be used to analyse large amounts of data and easily find anomalies. This helps detect security incidents at an earlier stage or before they become a serious problem. AI technology does not replace existing systems or experts, but rather reduces the amount of manual work required, quickens response times and thus improves the overall security of a company.

Which project are you currently working on?

We are developing a new platform to facilitate dialogue between our customers and us. Swisscom handles around 20 million customer interactions every year. The number is continuing to grow, as many customers typically use multiple channels seamlessly. High-quality service on all channels is therefore indispensable for an excellent customer experience. Customers should not have to re-enter their information when switching from one channel to the next. That is why Swisscom is setting up a new, AI-based dialogue platform to coordinate the different interaction channels and provide customers with the best possible support.

3.2 AI & ML applications in cyber security

As we showed in the status report for 2018, several trends are currently prompting the development and implementation of AI & ML solutions for cyber security measures.

- Increasing amounts of data and AI & ML applications; evaluations of these data could be abused to more efficiently make targeted attacks, for example.
- The trend toward shifting increasingly large amounts of assets into virtual space also motivates organised criminals even more to use new technologies to steal or compromise those assets.
- The ongoing rapid growth in the demand for cyber security experts is already making it difficult to train, integrate, develop and retain enough top talent. The situation will worsen significantly in the coming years.

3.2.1 Security Operation Centre

One mainstay of a sophisticated cyber security strategy is the ability to recognise that an attack has occurred. This task is performed by the Security Operation Centre (SOC).

One of the vital jobs of an SOC analyst is to differentiate relevant from non-relevant events (referred to as “false positives”) and to further treat only relevant events (“true positives”) as an incident or as a security incident. To perform these tasks, analysts are already using rule-based tools, for example. However, these tools are only as good as the rules defined in advance for their application. Consequently, their weakness is that they are not able to react quickly to changes and extraordinary, unforeseen incidents. As data volumes rise and attacks become smarter, rule-based tools will no longer be enough to protect businesses and their customers against attacks.

Smart, self-learning systems are the key to further developing the ability to prevent, or at least anticipate, attacks and ward attacks off. What is more, these systems are not only capable of independently detecting threats, but also of actively seeking out vulnerabilities in a system’s configuration and either proposing corrective measures or implementing them immediately.

3.2.2 Phisherman

At Swisscom, we are already using machine learning to address security threats. Phishing is a threat that affects our business and our customers every day. In phishing, criminals try to obtain user data such as passwords or credit card information through the use of fake e-mails.
The cornerstone of phishing prevention is to recognise fraudulent e-mails correctly and quickly and to distinguish them from real ones. Phishing attacks are becoming more targeted and professional, so even the most careful and tech-savvy users are not always able to clearly identify phishing attacks as such.
This is where machine learning delivers added value. Phishingman, our anti-phishing application, uses advanced machine learning techniques to identify and classify phishing attempts.

The following illustration shows a recent excerpt from Phisherman with a comparison of the 2016 and 2017 trends.
"Top phished companies" means that attackers have tried to impersonate the company specified in dealings with other individuals. This is most frequently attempted through fake e-mails. While the graph clearly shows that US companies and their customers were the main targets in 2016, a larger number of Swiss companies were affected in 2017. While Apple still leads the statistics and Swisscom came in fifth in both years, UBS and PostFinance were both hit hard for the first in 2017.

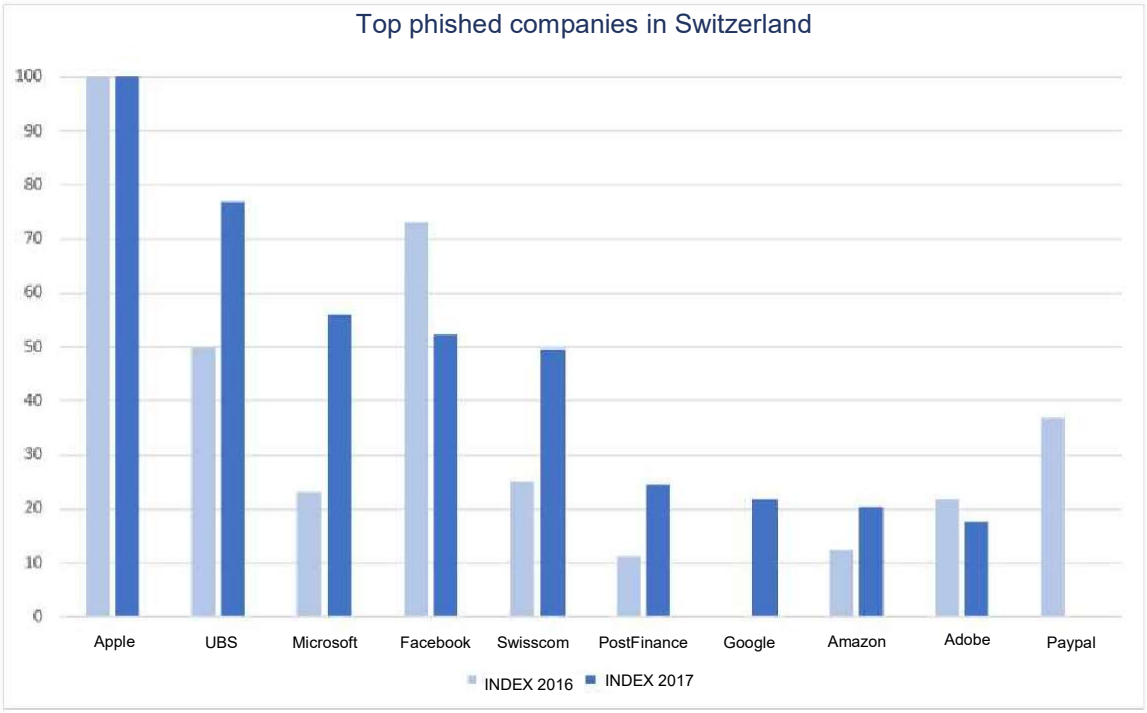

Figure 3: Top phished companies in Switzerland, 2016/17 analysis by Swisscom Phisherman

Based on this change, we can conclude that phishing attacks have become more targeted, smarter and, consequently, among other things, more regional. The closer

the attackers are to the real living environment of the individuals involved, the easier it is for them to deceive their victims and benefit from this deception.

3.3 Conclusion

The use of AI applications will be a key factor in cyber security in the short to medium term. As discussed above, security analysts are no longer capable of reasonably evaluating the steadily growing volumes of data using the existing support systems. Furthermore, the attacks are becoming increasingly smart and targeted. AI applications are needed to distinguish between critical and non-critical events, but these systems should only be used in a supporting role for the time being. Until AI has proven itself in everyday life over a longer period of time, decision-making responsibility must remain with specialists.

4. Implementation in the Swisscom network

With several million Internet access connections and as a provider of IT and telecommunications infrastructures for large companies, Swisscom is impacted heavily by a wide range of threats on a daily basis, which are aimed either at end customers or Swisscom's own infrastructures.

In order to provide an overview of these threats, we analysed data from DNS sinkholes (see Glossary) and passive DNS data over a period of six months. The detection analysis primarily considered DNS access when attributing threats for the end-user segment within the Swisscom network. One limitation with respect to the meaningfulness of this analytical method is that detection depends on whether the domain is known and has been recorded in the sinkhole data.

The results presented here are intended to provide an overview of the most important insights:

The analysis of the detected threats reveals a clear predominance of malware call-home traffic (command and control), while DNS amplification and adware are less frequent. Another dominant trend currently emerging is communication with crypto-mining infrastructures.

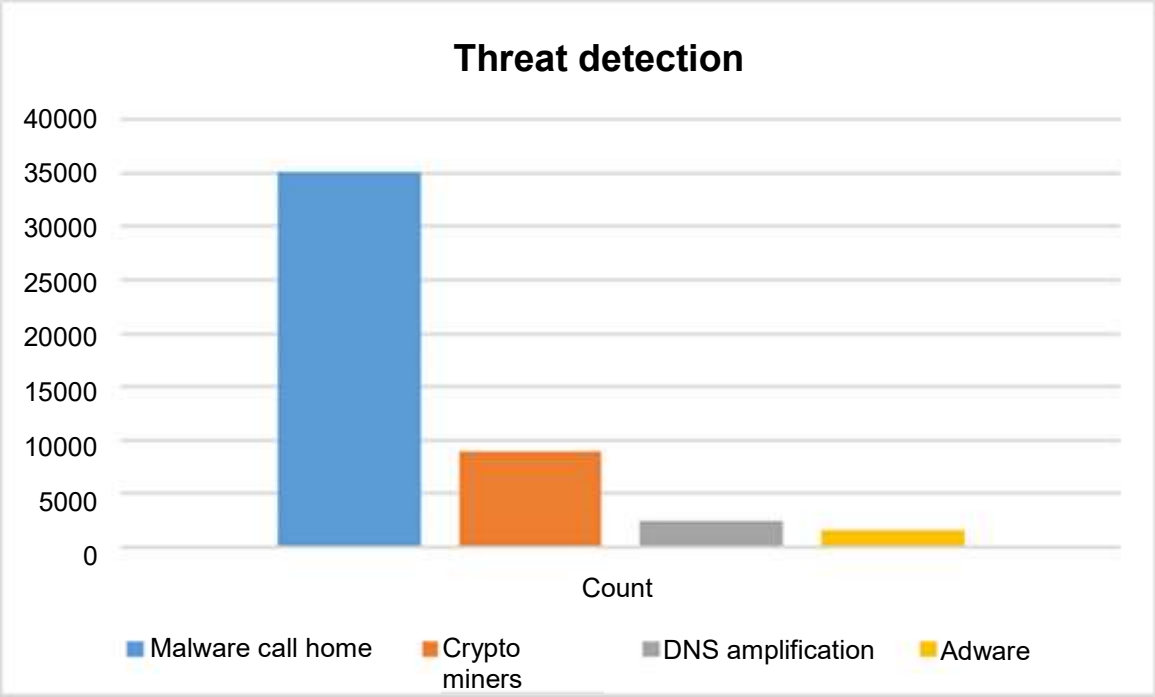

Figure 4: Threat detection

4.1 Malware call home

We use the term "malware call home" to refer to typical command-and-control (CnC) network traffic. Command-and-control refers to communication between an infected system (e.g. a bot) and the system controlled by an attacker. The attacker needs this channel in order to retain control of the affected system and carry out DDoS attacks, send spam e-mails or infect other systems, for example. Conficker, Ramnit and Gamut are found quite frequently within Swisscom's end customer network. Because ransomware often has no command-and-control component, detecting ransomware by means of DNS queries is difficult. An exception is the WannaCry ransomware, which can be detected through the kill switch domain.

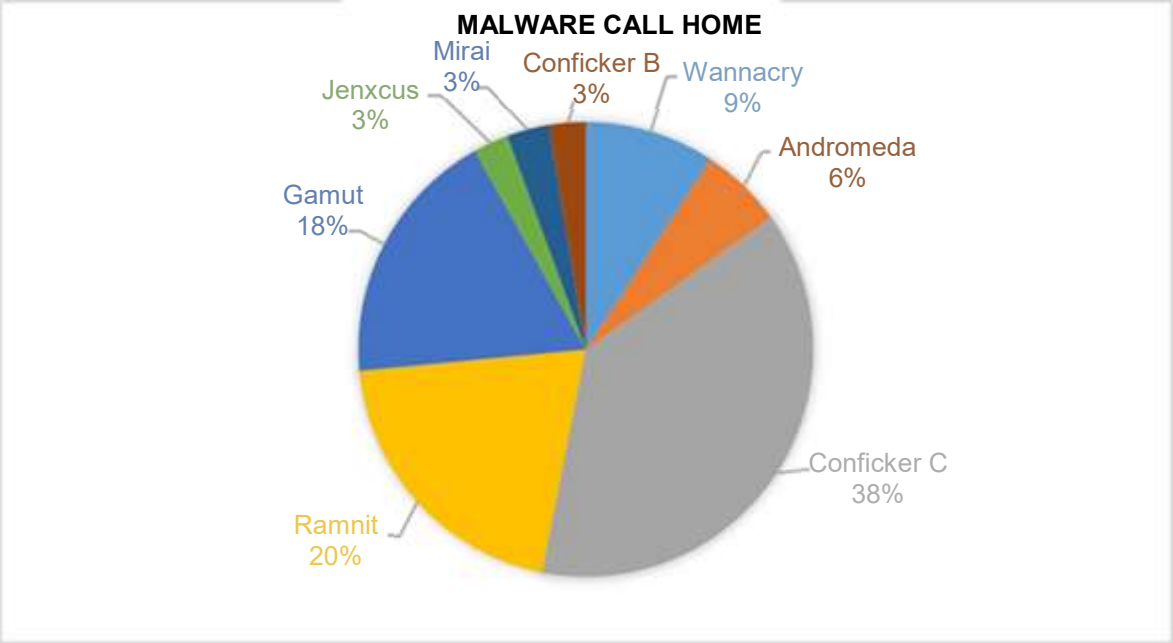

Figure 5: Malware call home

The results represent identified access attempts to previously blocked infrastructures via the DNS sinkholes.

Different versions of **Conficker**, also known as Downadup, have surfaced since 2008 and infected millions of Windows systems. This malware exploited a vulnerability in the server service of Microsoft Windows and, in its B and C versions, used a dictionary attack and exploitation of Windows Autorun to propagate itself. Version C is the most prevalent malware family found in Switzerland. A working group (Conficker Working Group) was set up explicitly for the purpose of stopping Conficker and was able to keep it from spreading any further. It is still unclear who is behind Conficker.

Ramnit is a modular malware toolkit that has been extremely popular among cybercriminals since 2010. This malware is able to track the web browsing behaviour of the victim systems and, for example, can read and exfiltrate any access data entered. The toolkit uses several methods to remain in an infected system. It infects .exe, .dll, .htm and .html files, among other things. The malware

copies itself to all connected hard drives (even devices connected via USB are infected). Ramnit infections are still very common in Switzerland.

Gamut is a spamming botnet that hijacks Windows systems to send spam. According to a recent analysis, Gamut, together with the spam botnet Necurs, was responsible for 97% of all spam e-mails sent during the last quarter of 2017.

4.1.1 WannaCry

Although WannaCry is reported less frequently on our network, we still want to address it because of the special nature of this ransomware. Previous forms of ransomware were characterised by spam e-mails, infected websites or botnets that infiltrated target systems and remained there to extort money from their victims. Ransomware is extremely popular, especially among cybercriminals. The table below lists what we feel are the main reasons for this:

Low entry barrier	A growing professionalisation of ransomware-as-a-service offerings, giving even criminals without programming skills or technical know-how the means of carrying out ransomware attacks.
Anonymous money transfers	The proliferation of anonymous cryptocurrencies like Monero, allowing cybercriminals to operate globally and extort digital money from their victims all around the world without being identified or tracked.
Helplessness of the victims	Especially private users and SMEs without a backup strategy for their data think that paying extortion money is the only way to get their data back.

WannaCry was the first to achieve a new dimension in automated ransomware infections. The WannaCry campaign, detected in May 2017, used the previously publicised ETERNALBLUE exploit from the leaked NSA arsenal. Within just days, more than 230,000 systems in more than 150 countries were automatically infected. Victims included critical infrastructures such as the National Health Service and Deutsche Bahn[1].

[1] https://www.heise.de/newsticker/meldung/Ransomware-WannaCry-befaellt-Rechner-der-Deutschen-Bahn-3713426.html

Figure 6: WannaCry infection

Switzerland was and continues to be affected by the WannaCry campaign, but, unlike in many other countries, critical infrastructures have not been affected. Globally, however, the attack shows that exploiting one single vulnerability via lateral propagation mechanisms can create a pandemic that blurs network boundaries, such as the perimeter and internal network, exposing the vulnerability of our networked systems and our digital age.

4.2 Crypto mining

While cryptocurrencies continue to be enormously popular in ransomware attacks, another new trend has emerged in the threats detected to Swisscom's network: cryptocurrency mining[2]. When we speak of cryptocurrency mining as a recognised threat, we are referring to the unauthorised mining of cryptocurrencies, e.g. through the unauthorised installation of miners by:

Insiders	A company's employees can be attracted by the opportunity to do mining for free using the company's resources (processing power) and at the company's expense (electricity). Employees with special privileges (e.g. administrators, power users) could exploit this[3].
Malware	Unlike ransomware which generates one-time payments, miners ensure regular income, making them far more lucrative for cybercriminals.
Drive-by mining	Drive-by mining takes place in the browser itself via scripts which exploit the CPU resources of visitors to the website.

A general evaluation of our passive DNS data shows which pools are actively being used to mine cryptocurrencies.

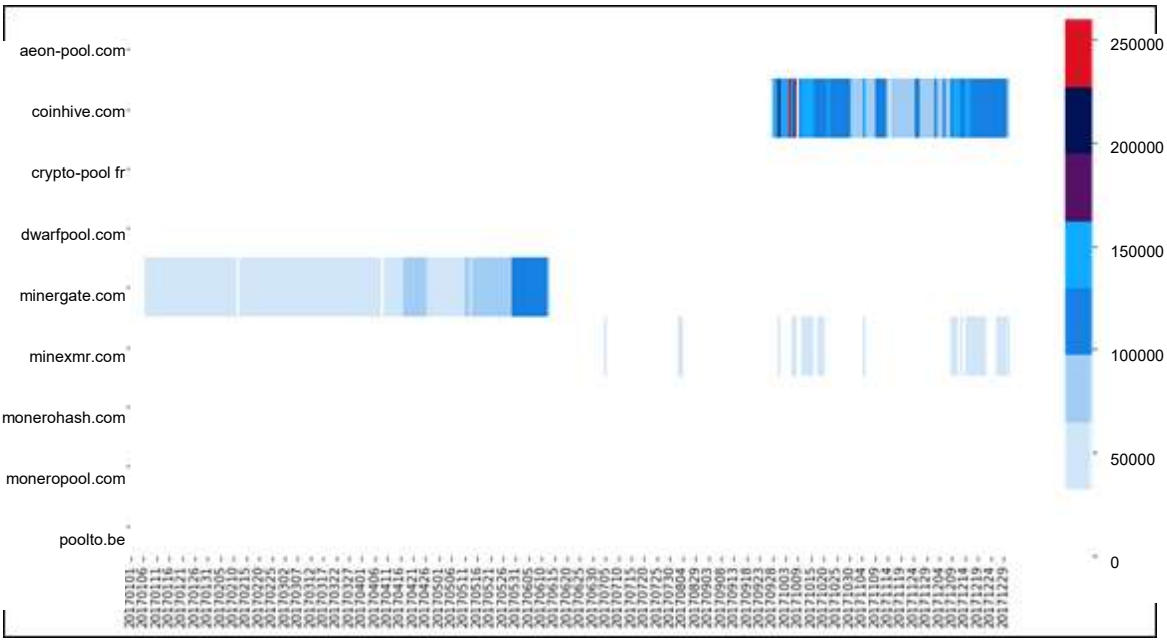

Figure 7: Mining pool usage

[2] When mining, processing power is used to confirm cryptocurrency transactions. Miners receive a financial incentive.
[3] https://www.rferl.org/a/russia-sarov-nuclear-facility-workers-arrested-using-supercomputer-mine-bitcoin/29030004.html

White spaces indicate that these pools account for fewer than 50,000 hits per day. The pools minergate.com and coinhive.com are particularly noteworthy. The use of these pools does not imply malicious intent per se; however, cybercriminals long ago began equipping their malware with cryptominers and fall back on established mining pools in this lucrative model for monetising infected computers.

The proliferation of installed miners affects clients, servers and browsers alike.

4.2.1 Coinhive

Coinhive, in particular, is hugely popular among attackers for mining cryptocurrencies via drive-by mining. Since Coinhive runs in a victim's browser and hijacks website visitors' CPU power via JavaScript to mine the cryptocurrency Monero, it is easy to use and generates no operating costs for the cybercriminals. In order to get the highest possible payouts, cybercriminals target highly frequented websites. Even government websites have long since become targets, where Coinhive mining JavaScript has been integrated and misused for carrying out drive-by mining attacks[4].

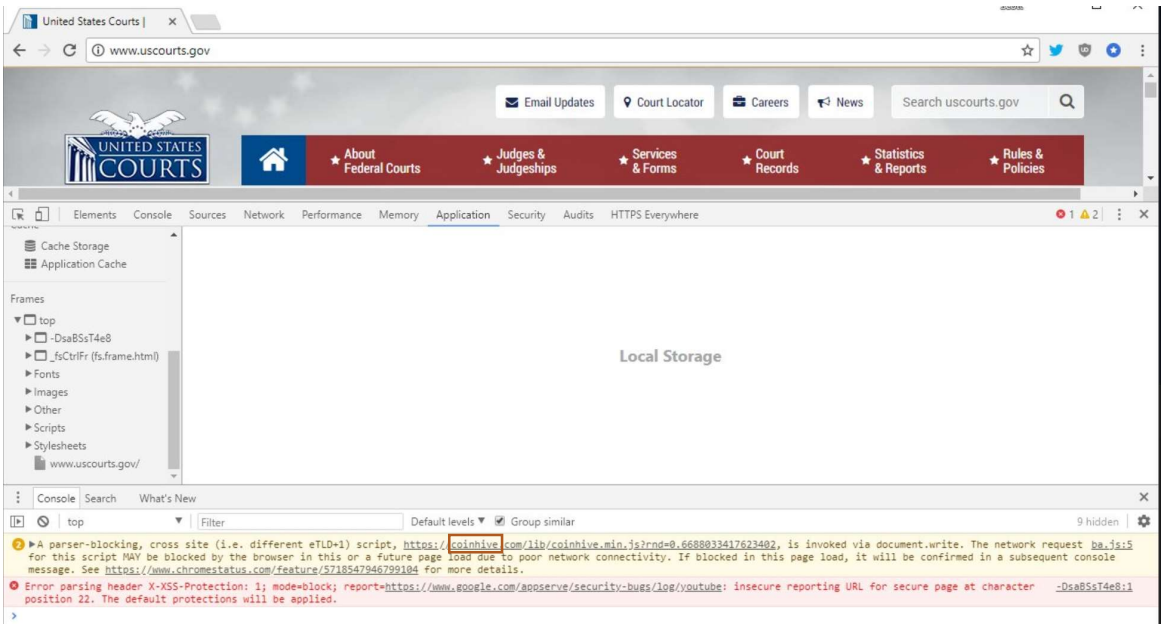

Figure 8: Website of the United States Courts infected with Coinhive JavaScript.

In a recent analysis, we used the website publicwww.com to identify websites that load the Coinhive JavaScript.

[4] https://twitter.com/Scott_Helme/status/962684239975272450

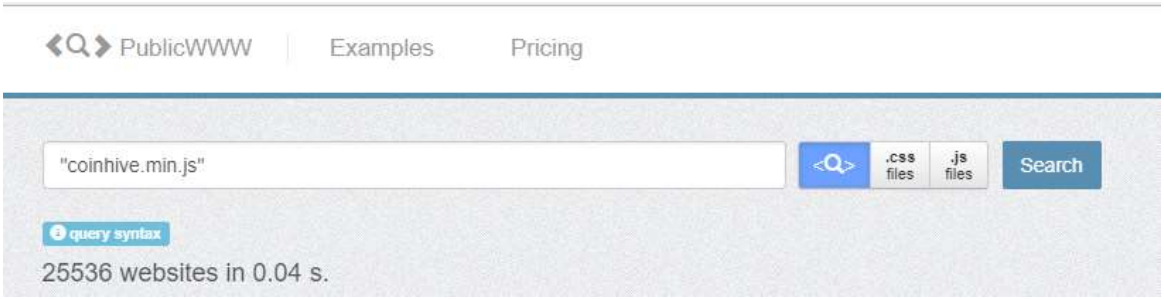

Figure 9: Coinhive on publicwww

In all, more than 25,500 websites were identified that perform Coinhive drive-by mining on the end devices of visitors to those sites. Many of these websites have been identified as compromised[5].

4.3 Conclusion

Conficker, Gamut, Ramnit and WannaCry infections among end users within the Swisscom network represent malware families with different purposes. Conficker infections indicate that many of the infected systems still use legacy operating systems that are susceptible to the vulnerability exploited by Conficker. The Gamut and Ramnit infections show that cybercriminals have taken control of a large number of Swiss end-customer systems and misuse them for their own purposes. Although Switzerland was impacted only little by WannaCry, we must still assume that with growing digitisation (see the Threat Radar) the risk of another "out-of-control" cyber weapon with global implications is increasing.

The evaluation of cryptocurrency mining pools has revealed that a large number of access operations could be attributable to drive-by cryptomining. The lucrative model and the anonymity of cryptocurrencies make this new technology particularly interesting for cybercriminals. In addition to miners being installed by insiders and drive-by mining like Coinhive, companies may also move on to leveraging existing enterprise resources for the purpose of mining.

As an Internet Service Provider, Swisscom guarantees smooth, barrier-free, secure Internet access for our customers and our society. We not only have an obligation to protect our customers, but we also need to ensure that we do not hamper the Internet's openness and that we promote an open Internet in Switzerland[6].

We already have different established mechanisms in place to ensure protection against malware, such as:

[5] https://badpackets.net/cryptojacking-malware-coinhive-found-on-30000-websites/
[6] https://asut.ch/asut/media/id/153/type/document/bv_verhaltenskodex_mit_asut_201603.pdf

Spam traps	Spam traps are e-mail addresses without users that were created for the purpose of identifying illegitimate e-mails like spam, phishing and malware attacks. Swisscom operates thousands of these e-mail accounts, whose contents are automatically analysed and incorporated into the protective filters.
Internet Guard	The Swisscom Internet Guard works on the basis of both third-party blacklists and its own blacklists, which are fed into our DNS servers and blocked. Use of the Internet Guard DNS infrastructure protects Swisscom customers against websites flagged as being malicious.
Customer reports	Fraudulent websites (e.g. phishing or attempted fraud), websites with malware (viruses, Trojan horses etc.) and those that exploit a security vulnerability on devices can be reported directly to spamreport@bluewin.ch by e-mail.

Customers who are already infected with malware are terminated in a sandbox – an isolated quarantine network. When attempting to connect to the Internet, they are shown an information page explaining what was done and why, and they are also provided with additional information and tips on how they can rectify the situation themselves. This block does not affect Swisscom TV or telephony. Other connections the customer needs to rectify the problem are also still enabled, such as antivirus programmes, software updates etc.

5. Glossary

0-day/zero-day exploit	A software exploit recognised the first time a security gap is published – or even beforehand. This means that the exploit is made available before the software manufacturer has a security patch at the ready.
API	Application Programming Interface. An interface that enables programmes to directly exchange data (machine to machine) using a common language.
Back door	Software back doors are used to gain access to a computer by circumnavigating its access protection.
Botnet	A network of a large number of compromised computers that are controlled centrally by a botmaster.
Defacement	Uploading unwanted content to a hacked website.
DoS, DDoS	Denial of Service (DoS). A large number of requests that causes a system to crash. Distributed Denial of Service (DDoS). The DoS attack is launched simultaneously from a large number of widely distributed systems (e.g. a botnet). It is no longer possible to simply block the attacker.
DNS sinkhole	DNS sinkholes are mainly used to direct a domain recognised as malicious to another IP address via DNS.
Exploit	Programme, code or a series of commands used to take advantage of vulnerabilities in software.
Exploit mitigation	A general term for techniques that make it harder or impossible to abuse system vulnerabilities.
ICS	Industry Control System. For more information, see SCADA.
ICT	Information and Communication Technology.
Jamming	The deliberate disruption of radio communications.
Kill switch	Hidden software that can disrupt or shut down the functioning of a system when given the command from afar.
Malware	Software that executes damaging, unwanted functions.
Money mule	Criminals convince people to take money from “clients” and, after having taken their cut, pass it on to a money transfer service. Money mules believe they are working for a legitimate organisation.
Monero	Monero is a cryptocurrency that offers specific advantages for cybercriminals, such as untraceable transactions and the CryptoNight algorithm that prefers the CPUs and GPUs of computers and servers. With respect to the latter, Monero is significantly different

	from Bitcoin in terms of mining, which now requires special, expensive hardware.
OSINT	Open Source Intelligence gathers information exclusively from sources that are accessible to the public.
Patch Security update.	Programming code that replaces defective software to eliminate security gaps.
Phishing	Users are tricked into disclosing sensitive data (using e-mails, giving fake instructions).
SCADA	Supervisory Control And Data Acquisition System Used to monitor and manage technical processes (e.g. industrial processes).
Vulnerability	A vulnerability or weak spot in hardware or software that attackers can use to gain access to a system.
SDR	Software Defined Radio. Universal high-frequency emitter and receiver that use software to process signals, which the user can adapt to different protocols and applications.
Smart grid	Intelligent power grid. The smart grid interconnects and manages electricity generation and storage, electrical appliances and energy transfer and distribution networks.
Smart home	The overarching term for networked, partially automated management of energy, entertainment and security in homes.
Social media	Websites that enable users to interact via personal profiles (e.g. Facebook, Twitter, LinkedIn, Xing).
Spear phishing	Targeted, personalised phishing attack, e.g. to get the access data of key persons.
Spoofing	Deceitful behaviour in networks intended to conceal the actor's identity.