



# CYBER-ATTACKS DETECTION AND PREVENTION



Co-funded by the  
Erasmus+ Programme  
of the European Union



Publication financed by the European Commission under the Erasmus + programme.  
The European Commission's support for the production of this publication does not constitute an endorsement  
of the contents, which reflect the views only of the authors, and neither the Commission nor the National Agency  
cannot be held responsible for any use which may be made of the information contained therein.

## Table of contents

1. Introduction
2. The concept of cybercrime and related concepts
  - 2.1. Cybercrime
  - 2.2. Classification of cybercrime forms
  - 2.3. Cyberattack
  - 2.4. SUMMARY
3. Criminal law protection against cybercrime
  - 3.1. Cybercrime in international and EC/EU documents
  - 3.2. Substantive aspects of cybercrime in Poland
  - 3.3. Substantive aspects of cybercrime in Portugal
4. Manifestations of cybercrime
  - 4.1. Social Engineering
  - 4.2. Botnet
  - 4.3. Malware
  - 4.4. Ransomware
  - 4.5. Spam
  - 4.6. Phishing, Pharming, Spear Phishing, Vishing, Smishing
  - 4.7. Business Email Compromise (BEC)
  - 4.8. Fraudulent websites (companies)
  - 4.9. Hacking
  - 4.10. Cracking
  - 4.11. Internet (computer) piracy
  - 4.12. Sniffing
  - 4.13. DoS, DDoS, DRDoS attacks
  - 4.14. Dissemination of defective content
  - 4.15. Cyberattacks on social networks
  - 4.16. Identity theft
  - 4.17. APT (Advanced Persistent Threat)
  - 4.18. Cyberterrorism
  - 4.19. SUMMARY
5. Conclusion
6. Reference list

# 1. Introduction

## LECTURES

1. Legal norms regulating cybercrime
2. Social engineering
3. Spam, Scam, Hoax
4. Botnet
5. Cyber attacks - Hacking, cracking, malware, ransomware
6. Cyber attacks - Financially focused attacks of the (phishing pharming, spear phishing, mobile phishing)
7. Cyber attacks - social attacks (cyberbullying, stalking, sexting, cybergrooming, etc.)

## WORKSHOPS

1. Analysis of individual cyber attacks and their subsumption under the provisions of the Convention on Cybercrime (ETS No. 185) and national law (Czech Republic, Poland, Portugal)
2. Analysis of individual attacks - modus operandi
3. Security testing against selected attacks.
4. Defining prevention options against individual types of attacks
5. Design of your own solution for protection against individual cyber attacks.
6. Security testing of some systems, applications and data. Students will try to design their own solutions to increase the security of these systems, applications or data.



## INTRODUCTION

At present, information and communication technologies are indispensable. Their contribution to society in all areas of human activity (e.g. medical science, research, security, transport, etc.) is indisputable. The field of information and communication technologies is the fastest and most proliferating branch of human activity.

What needs to be realised is the fact that information or data and their use involve considerable economic and political potential. Information, as both raw data and dataflow, can determine not only the existence or non-existence of an individual or company but also, by its nature, influence global development.

However, the use of information and communication technologies also has its downsides. One of them, undoubtedly, is the gigantic and dynamic increase in the "new type" of crime, which must be dealt with in such a way as not to endanger and violate the interests of society. This crime can be collectively called cybercrime.[\[1\]](#)

It should be noted that, on a global scale, considerable efforts can be observed, both at the legal and security levels, to take adequate measures to respond to this new and dynamic phenomenon of today.[\[2\]](#)

Three facts have become **key points for the development of cybercrime**.[\[3\]](#) The first is the connection of four university computers and the creation of a computer network for data sharing.[\[4\]](#) The second is the creation of IBM's first Personal Computer in the late 1980s. The third and, in my opinion, most important milestone is making the Internet accessible to the general public, including the modification of individual applications into a more user-friendly form.

The development of today's digital society is not based directly on economic development associated with material resources but on the development of IT, on connecting more and more users to the Internet, but especially on applications as such and last but not least on obtaining information and data from users themselves. These changes are connected to the development of IT, both socially and economically, and are one of the causes of cybercrime.

Cyberspace is currently the most effective and dangerous weapon in the hands of cybercriminals. It is not that cyberspace or the Internet itself is dangerous or lacking security. The point is that a system is always as strong as its weakest link. In this case, the weakest element is, more than ever, a user. In fact, a user is the biggest "threat" to himself/herself and his/her surroundings, because even though he/she has legal personality.[\[5\]](#), he/she often has only a minimal knowledge of his/her rights and obligations.

The Internet has become a part of our daily lives and especially its multimedia aspect is developing very fast. The Internet, whether we like it or not, is a more powerful and predatory medium than television or any other mass media. Nowadays, even a simple user can pass or force his/her thoughts or opinions onto the entire global population through a simple interface. And it doesn't matter if the thoughts are banal or perverted in some way.

On the one hand, the Internet offers virtually unlimited possibilities for almost anyone in obtaining and processing information about almost anything, without the need to spend time in libraries or information centres outside the home (obtaining the information in question is a matter of a few seconds).

Google and Wikipedia have become relevant and often the only sources of information for our decisions. The Internet enables communication between people, facilitates a number of activities thanks to the possibility of finding a solution or instructions, offers a number of different information channels, etc. At the same time, it allows you to do all this from your home and with a feeling of almost absolute anonymity.

On the other hand, working in this virtual environment can result in severe financial loss, fear of intrusions into your privacy by strangers, loss of valuable personal data, online communication of mentally disturbed people (paedophiles, drug addicts, philosophically adrift, etc.), communication of these people with our own children behind our backs, arranging criminal groups for illegal activities without the possibility of eavesdropping by a third party, fraud, unauthorised intrusions into private spheres of companies, redirection of business orders, theft of other people's accounts, destruction of data and databases, copyright infringement, etc.

Cyberspace cannot be allowed to become an environment where perpetrators could commit any criminality virtually without punishment. But there is only one starting point for fighting crime in cyberspace, and that is cyberspace itself. It is necessary to understand what cyberspace actually represents, what principles it works on, what types of crime can occur in this virtual world, and what all law enforcement agencies, but especially the user himself, can do against this illegal activity.

As already mentioned, cybercrime has been gaining momentum in recent times. Due to its varied nature, a wide range of each of our fundamental human rights is infringed, and information and communication technologies thus become the means by which crime is committed or are themselves the target of this activity.

A significant difference between cybercrime and other types of crime is its considerable latency, often a high level of tolerance by society (including user indifference to potential threats), real or perceived anonymity of the perpetrator and its difficult identification, as well as the whole process of proving. Therefore, it is necessary not only to address the issue of repressive action against offenders but also the issue of crime prevention in this area, as well as the issue of possible protection of society from this crime.

The actual prevention of these negative phenomena must necessarily begin with end users because in cyberspace it is they who are the typical first victim of an attacker. Based on my experience, I am convinced that the education and training of users should be an essential part of the penetration of information and communication technologies into our lives. I believe that building information literacy should be inextricably linked to the creation, distribution and promotion of products or services that are associated with information and communication technologies. The actual education in this area, or rather learning about possible threats, risks and drawbacks posed by IT, should be part of the teaching of all forms of study at all levels of education.

As far as people who deal with this issue at a professional level are concerned, then even higher demands are placed on these specialists, as they must constantly learn and train to be able to face ever new and dynamically growing attacks by ICT means and in the ICT environment.

---

[1] **Cybercrime** is often referred to by various names. I believe that cybercrime is the most apt term for this infringement. In this monograph, the terms **cybercrime**, **cybercriminality** or **cybercriminal activity** will also be used to refer to this phenomenon.

A definition of the differences between crime and criminal activity in this area will be included in the next part of this publication, as well as a definition of the views of various authors on the exact label for this criminal activity. The term cybercrime will be mostly used in this publication.

[2] For example: *Fight against cyber crime: cyber patrols and Internet investigation teams to reinforce the EU strategy*. [online]. [cit.10.7.2016]. Available from: <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1827>

[3] These facts were then supported by a number of other circumstances (e.g. lack of legislation in relation to the Internet, inability to enforce the law, the feeling of anonymity among users, etc.).

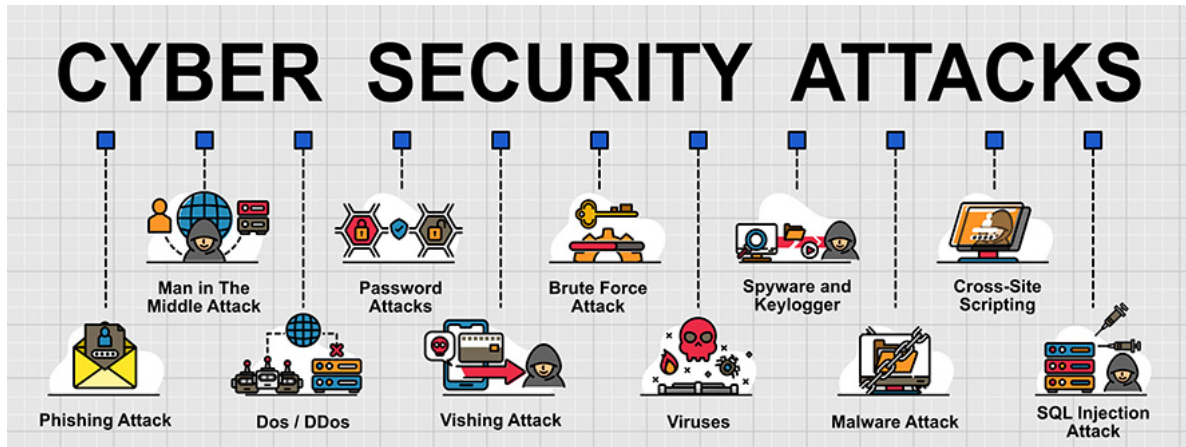
[4] For more details see ARPANET or NSFNET. It is the late 1960s.

Cf. *Historical Maps of Computer Networks*. [online]. [cit.10.7.2016]. Available from:

<https://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/historical.html>

[5] They have rights and obligations. Users establish, change and possibly terminate legal relationships.

## 2. The concept of cybercrime and related concepts



## 2.1. Cybercrime

Using computer technology, information systems and information technologies and their integration into almost all branches of human activity is a phenomenon that is characteristic of today. It can be stated that **in principle it is not possible to find such an area of human activity, where computer technology, or information system or information or communication technology, would not be used directly or indirectly.**

Unfortunately, as the possibilities of using these modern-day conveniences and scientific and technical progress increase, so do the possibilities and at the same time the frequency of their misuse to commit crime.

In the 1990s, the term "**computer crime**" (počítačovákriminalita, *Computerkriminalität*) became established for information technology crime. In his publication, Smejkal defines, in the mid-1990s, *computer crime* as a diverse mix of crimes whose common factor is the computer, program and data. The term computer crime "... is to be understood as committing a crime in which the computer as an aggregate of hardware and software, including data, or a large number of computers separate or connected to a computer network is central to either being the subject of such a crime, though with the exception of a crime where the mentioned device is the subject of the crime as simple property, or as instruments of crime."<sup>[1]</sup> It is clear from the above definition that computer crime related only to computer systems as targets of attack.

The term "computer crime" evokes the idea that a crime must be committed on a computer or through a computer, most often a personal computer (PC). Such an understanding is now simplistic, and at the same time reduces somewhat, in quantitative terms, the number of phenomena that can be included in the concept of crime committed by means of information and communication technologies. Many technical devices today, thanks to the implementation of microprocessors together with their miniaturisation, assumed the role of personal computers (PCs) a long time ago, without being called personal computers. These are hybrids performing various functions, which were previously performed by special devices. Modern technical devices enabling communication between them and their users and whose design is guided by the principle of *ALL-IN-ONE* are capable of much higher computing power than the most modern computing units from the first half of the 90s. And even these devices<sup>[2]</sup>, although not called computers, can be the target of crime or a means of committing it. For these reasons, the terms "computer crime" or "computer offence" are now almost non-existent in the scientific literature. Instead of the term "computer", the terms "information and communication technology" (ICT) and "ICT crimes" are used.

In 2000, the Council of Europe issued a definition of computer crime under the Statute of the Commission of Experts on Cybercrime: "*An offence against the integrity, availability or secrecy of computer systems or an offence in the traditional sense using modern information and communication technologies*"<sup>[3]</sup>

EU Council Framework Decision 2002/584/JHA on the European Arrest Warrant refers to "**computer-related crime**" as conduct directed against a computer or conduct where the computer is a means of committing a crime. The definition of cybercrime is also based on the wording of the European Arrest Warrant.

In international conventions, the term "**cybercrime**" is most often used for crime committed by means of information technology, and the use of this term has also been transferred from the normative area to the vocabulary of the professional public. The concept of cybercrime has a similar character to the concepts of "*violent crime*", "*juvenile delinquency*", "*economic crime*", etc. *Such terms refer to groups of offences having a certain common factor, such as the manner of execution, the person of the perpetrator (at least generically), etc. in essence, it can be a very diverse mix of offences, connected by a common factor (computer, program, data).*<sup>[4]</sup>

When defining the content of the concept of **cybercrime**, it is necessary to realise that along with the growth of the possibilities of using information and communication devices, the possibility of their use (abuse) to commit crime is also growing. Therefore, in essence, there is no universal, generally accepted definition that would fully affect the scope and depth of this concept.

One of the possible definitions of computer crime or cybercrime can also be found in the Cybersecurity Glossary<sup>[5]</sup>:

### **Cyber crime**

„Criminal activity in which a computer appears in some way as an aggregate of hardware and software (including data), or only some of its components may appear, or sometimes a larger number of computers either standalone or interconnected into a computer network appear, and this either as the object of interest of this criminal activity (with the exception of such criminal activity whose objects are the described devices considered as immovable property) or as the environment (object) or as the instrument of criminal activity (See Computer crime).“

### **Computer crime / Cyber crime**

“Crime committed using a data processing system or computer network or directly related to them.”

These two definitions show an effort to define all aspects of cybercrime, but the authors have been guilty of some inaccuracies. First, they use both terms synonymously, but in the definition of cybercrime, they ignore the factors that the computer is both a target and a means of attack. Similar problems associated with this actual definition of cybercrime can be found also elsewhere.

In an effort to define cybercrime, it is appropriate to make use of Council of Europe Convention No. 185 on Cybercrime of 23 November 2001.<sup>[6]</sup> However, this convention does not define the concept of cybercrime. It only defines the measures that should be adopted by a ratifying party at the national level. These substantive criminal law measures then define a rough framework of crimes that are considered cybercrimes. This framework (together with other crimes contained in the Council of Europe Additional Protocol No. 189 to the Convention on Cybercrime<sup>[7]</sup>) provides a basic scope for uniform legal unification of criminal offences that can be considered cyber, across countries. The actual, often very strict definition of the given crimes is rather beneficial as it does not limit the national (more detailed or elaborate) implementation of these crimes but, at the same time, guarantees the fulfilment of minimum requirements (standards) by all ratifying parties.

Also due to considerable disagreement on what is and what is not cybercrime, in the following part of this chapter we will define this concept, both in terms of positive and negative.

In the most general terms, cybercrime can be defined as **conduct directed against a computer, or computer network, or as conduct in which a computer is used as a tool to commit a crime.** An indispensable criterion for the application of the definition of cybercrime is the fact that the computer network, or cyberspace, is then the environment in which this activity takes place.

When defining the concept of cybercrime, it is first necessary to **define the concept of crime in general.** Concerning the use of information systems, computer technology or communication devices, there are a number of actions that are certainly undesirable, but are not punishable under criminal law, although they can be very dangerous (harmful) for society. Such actions *a priori* cannot be qualified as computer, informational or any other crime – they are not crimes at all. When defining the term of criminality (and this definition can be given from several points of view – sociologically, criminally, etc.), we rely on the definition of criminality as a **summary of all actions that can be classified under an objective element, regulated by criminal law.** **Therefore, based on this definition, criminality does not involve such acts which do not meet any objective element of a criminal offence, i.e. not even a misdemeanour or other administrative offence.** Such a definition of the term criminality is relatively precise and can be used in the field of information and communication technology.

However, it is a characteristic of committing ICT crimes that such practices or means are used when committing them, the use of which does not fulfil any objective element of a crime, but are an integral part or prerequisite for engaging in criminal behaviour.<sup>[8]</sup> In addition, these non-criminal practices or means are important components in the process of uncovering and shedding light on crime, the identification and understanding of which plays an important role in detecting perpetrators of this type of crime.<sup>[9]</sup>

Cybercrime represents the broadest set for all crimes that occur in the information and communication technology environment. Offences committed within this set can be further classified and labelled with different terms according to various aspects. "Internet crime", "e-crime", "cyberterrorism" or, for example, "piracy" can then form subsets of cybercrime, though this list does not exhaust the possible subsets of actions that can be classified as cybercrime.

Cybercrime is most often used in professional publications to describe such criminal **acts in which the means of information and communication technologies are:**

- a) **used as a tool for committing a crime,**
- b) **the target of the offender's attack,** which is an offence.

**However, such a definition of cybercrime is no longer valid today.** This would include crimes involving the use of information technology but not in the context of their normal use or intention (e.g. cases where an offender injures a person by hitting a monitor or other part of the computer over the injured party's head with the intent to cause personal injury; or in the case of a theft of a truck carrying computer components, etc.). These are crimes where ICT is used beyond its intended purpose – for example, as a weapon, as a thing that has a certain monetary value, regardless of the purpose for which it is or should be intended. When uncovering and shedding light on these acts, other investigative methodologies (such as theft investigation methodology, etc.) will be used, not cybercrime investigation methods.

In order to talk about cybercrime, information and communication technologies that have been used to commit a crime or that have been the target of such a crime must be put into context. In this spirit, it is therefore necessary to assign another point containing this condition to the two above points. Cybercrime, then, is a crime where the means of information and communication technologies are:

- a) **used as a tool for committing a crime,**
- b) **are the target of the perpetrator's attack, and said attack is an offence,**

**provided that these devices are used or misused in an information, system, program or communication environment (i.e. in cyberspace).**

However, such a definition of cybercrime is still inadequate. Using the criteria set in this way to determine whether or not a specific conduct can be considered cybercrime, we conclude that, for example, aspects of defining participation (organisation, guidance and assistance) in the sense of Section 24 of Act No. 40/2009 Sb., Criminal Code, as amended,<sup>[10]</sup> it is possible to commit any intentional crime through information means (e.g. a person causes another person to commit an intentional murder crime by e-mail). It will be similar for other forms of criminal cooperation (e.g. incitement, endorsement of a crime). These can also be committed using information technology. **However, such actions cannot be described as cybercrime. As a result, accepting the opposite view would lead to the only possible conclusion – any crime in which an offender used information and communication technology in any way is a cybercrime.** From this point of view, it would be difficult to find crimes that cannot be considered cybercrime.

**It follows from the above that it is not enough to define cybercrime only positively, but it is also necessary to define it by a list of actions that cannot be considered cybercrime in principle.**

In this spirit, it will be possible to include crimes of three different categories under the term cybercrime:

- 1) crimes where the individual object characterising the objective element is directly the protection of the computer system, its equipment and components against specific types of attack or the legitimate interests of persons in the uninterrupted use of these technical devices,
- 2) crimes that are committed by means of information and communication technology is one of the features of the objective element,
- 3) other eligible crimes which do not fall into either the first or the second category, but which may also be committed in the specific case by means of information technology and which meet the above definition because similar detection procedures as when investigating of crimes from the 1st and 2nd category (e.g. similarly focused expert opinions) may be used to uncover and shed light on them.

---

[1] SMEJKAL, Vladimír, Tomáš SOKOL and Martin VLČEK. *Počítačové právo*. Prague: C. H. Beck, 1995, p. 99

[2] Currently, there are a number of devices, which are referred to as a computer system.

[3] MATĚJKA, Michal. *Počítačová kriminalita*. Prague: Computer Press, 2002, p. 5

[4] Smejkal, Vladimír. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015, p. 19

[5] JIRÁSEK, Petr, Luděk NOVÁK and Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. [online]. 2nd updated edition. Prague: AFCEA, 2015, p. 57 and 73. [online]. [cit.10.7.2016]. Available from: <https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovník-kyberneticke-bezpecnosti---druhe-vydani/>

[6] Hereinafter referred to as the **Convention on Cybercrime**. For more details, see <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>

[7] Hereinafter referred to as the **Additional Protocol**. ETS No. 189 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems

For more details, see <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189>

[8] For example, sending spam. Sometimes spam can only be an advertising (business) message. Such conduct is not punishable under criminal law. One can imagine, for example, sending SPAM for political, religious or other reasons. At other times, SPAM may contain malware that allows you to obtain a username and password to the client's bank account (which in certain circumstances can be qualified, for example, as preparation for a crime).

[9] For example, when the perpetrator communicates with his surroundings, it is possible to trace the IP address of his PC and then locate the location of the perpetrator's connection to the Internet.

[10] Hereinafter referred to as the **Criminal Code** or **CC**.



## 2.2. Classification of cybercrime forms

I believe that if we want to address the issue of cybercrime, it would be appropriate to at least define the parameters that delineate this crime. At the end of this subchapter, I want to present to the reader some classifications of cyber (or computer) crime as perceived by different procedural rules and various authors or organisations that are engaged in the fight against cyber crime. I also want to demonstrate in these categories the genesis of the view of the issue of cybercrime.

### **1. Classification according to the Convention on Cybercrime and according to the Additional Protocol.**

The Convention on Cybercrime divides cybercrime into four categories:

1. **Offences against the confidentiality, integrity and availability of computer data and systems,**
2. **Computer-related offences,**
3. **Content-related offences,**
4. **Offences related to infringements of copyright and related rights.**

The Additional Protocol then defines other cybercrimes:

1. **Dissemination of racist and xenophobic material through computer systems,**
2. **Racist and xenophobic motivated threat,**
3. **Racist and xenophobic motivated insult,**
4. **Denial, gross minimisation, approval or justification of genocide or crimes against humanity.**

### **2. Classification of the Committee of Experts on Crime in Cyberspace**

According to the Statute of the Council of Europe's Committee of Experts on Crime in Cyberspace from 2000, cybercrime can be divided into:

#### **1. According to position of the computer when committing a crime:**

- *target of the attack;*
- *means (tool) of the attack.*

#### **2. According to type of act:**

- *traditional infringements* (such as counterfeiting, etc.)
- *new infringements* (such as phishing, DDoS etc.)

### **3. Classification according to eEurope+**

This document divided computer crimes into:

#### **1. Crimes that violate privacy**

- Illegal collection, storage, modification, disclosure and dissemination of personal data.

#### **2. Crimes related to computer content**

- Child pornography, racism, incitement to violence, etc.

#### **3. Economic**

- Unauthorised access, sabotage, hacking, virus transmission, computer espionage, computer forgery and fraud.

#### **4. Crimes related to intellectual property<sup>[1]</sup>**

### **4. Classification of computer crime according to criminology**

Porada a Konrád<sup>[2]</sup> divide cybercrime into five basic groups.

#### **1. Unauthorised tampering with input data**

- change of input document for computer processing,
- creation of a document containing false data for subsequent processing of data by computer,

#### **2. Unauthorised changes to stored data**

- manipulation of data, unauthorised tampering with them and subsequent return to normal,

#### **3. Unauthorised instructions for computer operations**

- direct instruction to perform the operation or to install the software performing the operations automatically,

#### 4. Unauthorised intrusion into computers, computer system and its databases

- informative access to the database, without the use of information,
- unauthorised use of information for personal use,
- changes, destruction or replacement of information by others,
- illegal "interception" and recording of electronic communications traffic,

#### 5. Attack of another's computer, software and files and data in databases

- creation of attack programs,
- introduction of a virus into the computer software,
- infection by viruses or other programs.

#### 5. Europol's focus on certain types of cybercrime by severity

Europol respects the Convention on Cybercrime and abides by the breakdown of the offences contained therein. The European Cyber Crime Centre (EC3)<sup>[3]</sup> has been set up within Europol to support the fight against cybercrime and assist Member States. This team has clearly stated its scope of activity in the fight against cybercrime and has identified the following three areas (focal points – FPs) it deals with:

1. **FP TERMINAL – Payment fraud.** A group dedicated to providing support in online fraud.
2. **FP Cyborg – High-Tech Crimes.** A group dedicated to and providing support for various cyberattacks affecting critical infrastructure<sup>[4]</sup> and information systems. In particular, these are attacks such as: malware, ransomware, hacking, phishing, identity theft etc.
3. **FP Twins – Child Sexual Exploitation.** A group dedicated to and providing support in the investigation of child sexual abuse.

#### 6. Classification of cybercrime according to its "relationship" to the digital environment

With the development of cybercrime as such, an opinion has come to the forefront in recent years that propounds the possibility of viewing cybercrime as an act that could be described as "pure" or "genuine" cybercrime. Only those cyberattacks that took place in cyberspace and whose goal and tool was a computer system or data could be subsumed under such conduct. Typically, these are attacks identified as hacking, DoS, DDoS attacks, attacks on critical infrastructure, etc.

Other crime committed in the cyberspace environment is only considered as the transfer of "old" or "ordinary" criminal conduct into the new digital environment.

According to the above division, it would then be possible to understand cybercrime in a:

- Narrow concept ("pure" cybercrime);
- Broad concept ("ordinary" criminal conduct in a new environment).

#### Other possible classifications of cybercrime

There are many other methods of classification, to illustrate another possible division of cybercrime.<sup>[5]</sup>

At this point, I would like to mention my classification based on my own findings obtained especially in the interpretation of cybercrime at various seminars or conferences.

In a simplified way, it can be stated that cybercrime can be viewed from three perspectives:

##### 1. According to the frequency (nature) of attacks:

- a) **copyright infringement** (see Internet (computer) piracy. Within cyberspace, this act involving the infringement of intellectual property prevails. Efforts to combat this phenomenon are particularly evident on the part of private copyright organisations.);
- b) **other cyberattacks** (see manifestations of cybercrime. Except Internet (computer) piracy.).

##### 2. According to punishability by criminal law:

- a) **conduct resolved by criminal law** – some of the mentioned acts subsumable under the objective element of crime;
- b) **conduct not addressed (unpunishable) by criminal law** – some of the mentioned acts cannot be subsumed under the legal objective elements of the criminal offence, even using an admissible analogy<sup>[6]</sup>).

##### 3. According to the degree of tolerance by the majority society:

- a) **conduct tolerated by society** (copyright infringement conduct is most tolerated);
  - b) **conduct not accepted by society** (e.g. child pornography, etc.).
-

[1] For more details: JIROVSKÝ, Václav. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Prague: Grada, 2007, p. 92

[2] For more details: STRAUS, Jiří et al. *Kriminalistická metodika*. Plzeň: Aleš Čeněk, 2006, pp. 272–274

[3] *Combating Cybercrime in a Digital Age*. [online]. [cit.7.5.2018]. Available from: <https://www.europol.europa.eu/ec3>

[4] Regarding the definition of the term critical infrastructure, in the Czech Republic (in the case of cyberspace) it is necessary to proceed from the Act on Cybersecurity and on the amendment of related acts (the Act on Cybersecurity). Hereinafter referred to as the **Act on Cybersecurity**, or **AoCS**. In Section 2 (b), this act defines the term of critical information infrastructure and the critical infrastructure element or system.

The definition of the term “critical information infrastructure” is based on the legislation governing the area of crisis management. Critical information infrastructure is a part of critical infrastructure, which is defined by Act No. 240/2000 Sb., on Crisis Management and on Amendments to Certain Acts (Crisis Act) as amended (hereinafter referred to as the “Crisis Management Act”). In order to be included in the critical information infrastructure, a certain information system or service and electronic communications network must meet the definition criteria of the critical infrastructure as well as the critical infrastructure element defined by the Crisis Management Act and the cross-sectional and branch-specific criteria set by Government Decree No. 432/2010 Sb., on the Criteria for Determining the Critical Infrastructure Element.

Point VI has been inserted in the branch-specific criteria for determining the critical infrastructure element since the effectiveness of the act and cybersecurity. “*Communication and information systems*”, G: *cybersecurity*. Branch-specific criteria for the identification of a given information system, service or electronic communications network by a critical information infrastructure are set here.

However, this definition only applies to the area of cybersecurity. In general, **it is possible to define critical infrastructure as follows**:

1. Critical infrastructure means an element of critical infrastructure or a system of elements of critical infrastructure disruption, the function of which would have a significant impact on the security of the state, the provision of basic living needs of the population, human health or the state economy.
2. Element of critical infrastructure means a building, facility, tool or public infrastructure determined according to cross-sectional and branch criteria, which are set by Government Decree No. 432/2010 Sb., on Criteria for Determining the Element of Critical Infrastructure.
3. The cross-sectional criterion for determining the critical infrastructure element is the aspect of
  - a) victims with a threshold of more than 250 deaths or more than 2,500 persons with subsequent hospitalisation for more than 24 hours,
  - (b) an economic impact with the state’s economic loss threshold higher than 0.5% of gross domestic product, or
  - (c) an impact on the public with a threshold of a large-scale restriction on the provision of essential services or other serious interference in the daily life of more than 125,000 people.

[5] Cf. PROSISE, Chris and Kevin MANDIVA. *Incident Response & Computer Forensic, second edition*. Emeryville: McGraw-Hill, 2003, p. 22 et seq.

Then e.g. *CyberCrime*. [online]. [cit.1.2.2015]. Available from: <http://www.britannica.com/EBchecked/topic/130595/cybercrime/235699/Types-of-cybercrime>; etc.

[6] **Analogy means subsuming a case not explicitly stated in the criminal law under a similar statutory provision, specified in the law**. In contrast to the wider interpretation, a provision is used by analogy which, according to its meaning, does not apply to the subsumed case. A wider interpretation is made in accordance with the purpose of the criminal law and within its limits, while the analogy goes beyond these imaginary boundaries. By using an analogy, **gaps in the laws are filled**. It deals with cases that a legislator failed to regulate by a legal norm. Within the Czech and Portugal context, **they cannot be used to the detriment of an offender** (*in malam partem*).

## 2.3. Cyberattack

Prosis and Mandiva characterise a “**computer security event**” (which can be understood as a computer attack or computer crime), as an illegal, unauthorised, unacceptable action that involves a computer system or computer network. Such an action may focus, for example, on the theft of personal data, spam or other harassment, embezzlement, dissemination or possession of child pornography, etc.<sup>[1]</sup>

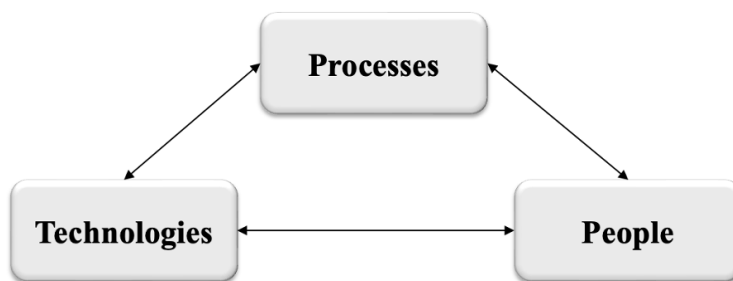
Jirásek et al. define a cyberattack as: “An attack on an IT infrastructure to cause damage and obtain sensitive or strategically important information. It is most often used in the context of politically or militarily motivated attacks.”<sup>[2]</sup>

Such a definition of a cyberattack would significantly narrow and not affect all the negative activities of cyberspace users<sup>[3]</sup>, especially because it cumulatively combines the conditions for IT damage and information retrieval. A cyberattack can also include actions in the form of social engineering, where the only goal is to obtain information, or, conversely, a DoS or DDoS attack, where the only goal may be to suppress (i.e. not damage) the functionality of one or more computer systems or services.

Based on the above, a **cyberattack**<sup>[4]</sup> can therefore be defined as **any illegal conduct by an attacker in cyberspace that is directed against the interests of another person**. These acts do not always take the form of a crime. Their essential characteristic is that they disrupt the injured party's normal way of life. A cyberattack counts whether completed, in preparation or at a trial stage.<sup>[5]</sup>

A cybercrime must also be a cyberattack, but not every cyberattack must be a crime. Many cyberattacks, even due to the absence of a criminal law standard, can be subsumed under conduct that will be by its nature an administrative or civil tort, or it may not be conduct that is punishable by any legal standard. (It can be, for example, only an immoral or unwanted conduct.)

The success of a cyberattack typically lies in the breach of one of the elements that make up cybersecurity (**people, processes, and technologies**). **These elements need to be applied or modified throughout their life cycle. In particular, they concern prevention, detection and response to attack.** The security of IT, information and data is also directly dependent on respecting the principles of “C”, “I” and “A”.



Elements of cybersecurity

If we want to define the term cyberattack, it is appropriate to use the definitions that result from Act No. 181/2014 Sb., on Cybersecurity and on the Amendment of Related Acts (Act on Cybersecurity).<sup>[6]</sup> This Act defines in Section 7 the terms of cybersecurity event and cybersecurity incident.

**Cybersecurity event** is “an event that may cause a breach in information security in information systems or a breach in security of services or security and integrity of electronic communications networks.” In fact, it is an event without a real negative consequence for a given communication or information system. In essence, it is only a threat, but it must be real.

**A cybersecurity incident** is “a breach in the security of information in information systems or a breach in the security of service provision or a breach of security and integrity of electronic communication networks due to a cybersecurity event.” A cybersecurity incident thus represents a real breach of information security in information systems or a breach in the security of services or the security and integrity of electronic communications networks, i.e. a breach of an information or communication system having a negative impact.

[1] PROSISE, Chris and Kevin MANDIVA. *Incident Response & Computer Forensic, second edition*. Emeryville: McGraw-Hill, 2003, p. 13

See also: CASEY, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Second Edition*. London: Academic Press, 2004, p. 9 et seq.

[2] JIRÁSEK, Petr, Luděk NOVÁK and Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. [online]. 2nd updated edition. Prague: AFCEA, 2015, p. 59. Available from: <http://afcea.cz/cesky-slovník-pojmu-kybernetické-bezpečnosti/>

[3] The above definition especially lacks a definition of any motivation of the attacker other than that... *causing damage or gain to strategically important information*. An example not covered by this definition can be economically motivated attacks, which are dramatically growing at present.

[4] It is necessary to distinguish the concept of a cyberattack from the concept of a **security incident**, which represents a breach of IS/IT security and the rules defined for its protection (security policy).

[5] E.g. Conficker virus attack created by Botnet. This completed the attack. However, the question remains as to what purposes this network may be used for. (It may be in preparation for a much more serious cyberattack.)

[6] Hereinafter referred to as the **Act on Cybersecurity**, or **AoCS**.



## 2.4. SUMMARY



### MAIN OUTPUTS FROM THE CHAPTER

- To understand the issue of cyberattacks and cybercriminality, it is necessary to know the basic terminology that is directly related to the selected area. This chapter presents selected technical as well as legal terms.
- It is not possible to find an area of human activity, where computer technology or rather information-system, information or communication technology would not be used directly or indirectly.
- The concept of cybercrime has a similar character to the concepts of "violent crime", "juvenile delinquency", "economic crime", etc. Such terms refer to groups of offences having a certain common factor, such as the manner of execution, the person of the perpetrator (at least generically), etc. In essence, it can be a very diverse mix of offences, connected by a common factor (computer, program, data).
- Cybercrime can be defined as conduct directed against a computer or, in some cases, computer network, or as conduct in which a computer is used as a tool to commit a crime. An indispensable criterion for the application of the definition of cybercrime is the fact that the computer network, or cyberspace, is then the environment in which this activity takes place.
- Cybercrime represents those criminal acts where the means of information and communication technologies are:
  - o used as a tool for committing a crime,
  - o the target of an offender's attack, which is an offence.
  - o provided that these devices are used or misused in an information, system, program or communication environment (i.e. in cyberspace).
- It is not enough to define cybercrime only positively, but it is also necessary to define it by a list of actions that cannot be considered cybercrime in principle.
- A cyberattack can be defined as any illegal conduct by an attacker in cyberspace that is directed against the interests of another person.
- Cybersecurity event is *"an event that may cause a breach in information security in information systems or a breach in security of services or security and integrity of electronic communications networks."*
- Computer data means *"any expression of facts, information or concepts in a form suitable for processing in a computer system, including a program capable of causing a computer system to perform a function."*
- Information *"is data that has been processed into a form useful to a recipient. So every piece of information is a piece of data, but any stored data doesn't necessarily become information."*



### KEY WORDS TO REMEMBER

- cybercrime
- cyberattack
- cybersecurity event
- crime
- cyberspace



### KNOWLEDGE CHECK QUESTIONS

- What is cybercrime?
- What is not cybercrime?
- What is a cyberattack?
- What is the difference between cybercrime and cyberattack?
- What is the difference between data and information?
- What is the CIA triad?

### 3. Criminal law protection against cybercrime

Efforts to regulate law and punish criminal activity committed by means of information and communication technologies can be virtually observed from the very beginning of these negative activities. Cybercrime is very different from other types of crime, and this difference lies mainly in the possibility of its dynamic development and immediate change (according to the success or failure of any type of attack), which can bring certain problems in relation to legislation.

In substantive criminal law, the principle applies that it is not possible to use analogy to the detriment of an offender (*in malam partem*). Nevertheless, cyberattacks can often be subsumed under a legal provision of a specific objective element, although this factual nature originally aimed at "more traditional ways" of committing a crime (typically attacks such as copyright infringement, child abuse for pornography, etc.). However, there are a number of new attacks for which this possibility is out of the question. In such cases, national legislators have so far primarily sought to respond on an *ad hoc* basis to these new types of crime, thus filling in the gaps in national legislation.

Before the actual analysis of the current valid and effective legislation in the field of cybercrime, it should be noted that there is a clear effort to implement more effective legal instruments, and not only within the European Union, that would be able to respond in a timely and adequate manner to cybercrime. This gradually eliminates inconsistencies and shortcomings in the legal norms of EU Member States and other states that have decided to become actively involved in the fight against cybercrime.

One of the first documents on cybercrime adopted at the international level is the **United Nations Manual on the prevention and control of computer-related crime** (Havana, 1990).<sup>[1]</sup>

*"Methods of protection of data and information systems are the subject of many scientific studies today. However, without a legal basis, the technical protection of these systems and data may be ineffective due to the unclear definition of how far it is possible to go with such protection. In this context, the inconsistency of the legal regulations of individual states with the legal regulations of other states is fully manifested. Thanks to the development of computer and information technologies, which indicate the international character of cybercrime, effective protection of computer systems and data is unthinkable without the existence of an international or transnational legal framework, not only between EU Member States, but worldwide."*

---

[1] *United Nations Manual on the prevention and control of computer-related crime*. [online]. [cit.20.8.2016]. Available from: [http://216.55.97.163/wp-content/themes/bcb/bdf/int\\_regulations/un/CompCrims\\_UN\\_Guide.pdf](http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_UN_Guide.pdf)

### 3.1. Cybercrime in international and EC/EU documents

The Convention on Cybercrime and its associated Additional Protocol should be mentioned first as these are the two most important legal documents that contribute to the protection of society against cybercrime by setting out a basic framework for cybercrime and at the same time providing the means to detect and investigate it. EU and EC legal documents related to cybercrime will also be presented.

#### 3.1.1 Council of Europe Convention No. 185 on Cybercrime

The Convention on Cybercrime is the most important legal document on cybercrime. Its main purpose is to unify national legislation in the field of cybercrime. The above is implemented by the fact that the Convention on Cybercrime obliges the contracting parties to implement into national legal systems such instruments that will enable the punishment of defined cybercrimes. It is the thorough definition of the objective element of crime that is a condition for the use of the rules of criminal law in cyberspace. Furthermore, the Convention on Cybercrime creates a legal framework for uniform and joint action against the perpetrators of these crimes, regardless of the place where the crime was committed.

The Convention on Cybercrime was approved by the Committee of Ministers of the Council of Europe at its 109th meeting on 8<sup>th</sup> November 2001. The Convention on Cybercrime was opened for signing on 23<sup>rd</sup> November 2001 in Budapest. [1] This convention entered into force on 1<sup>st</sup> July 2004.

The Czech Republic signed the Convention on Cybercrime on 9<sup>th</sup> February 2005 and ratified it on 22<sup>nd</sup> August 2013, coming into force on 1<sup>st</sup> December 2013, while Portugal signed at the first day, but only ratified it the 24<sup>th</sup> March 2010, entering into force the following 1<sup>st</sup> July. EU Member States have committed themselves to ratifying the Convention on Cybercrime and incorporating such provisions into their legal systems, which would make it possible to clarify and investigate said criminal activity. [2] The Convention on Cybercrime has also been signed and ratified, for example, by the United States, Japan and others.

The Convention on Cybercrime [3] consists of a **preamble** and **48 articles**, which are divided into 4 chapters:

##### 1. Use of terms

##### 2. Measures to be taken at the national level

**Part 1 – Substantive criminal law** (Articles 2–13)

**Part 2 – Procedural law**(Articles 14–21)

**Part 3 – Jurisdiction**(Article 22)

##### 3. International co-operation

**Part 1 – General principles**(Articles 23–28)

**Part 2 – Specific provisions**(Articles 29–35)

##### 4. Final provisions

An important step towards the unification of law is the definition of four basic groups of criminal offences (see Chapter II; Articles 2–13) and the anchoring of other general institutes of substantive criminal law. It is the uniform definition (naming) of cyberattacks that will enable their more effective prosecution in countries that have ratified the Convention on Cybercrime. In particular:

- 1) **Offences against the confidentiality, integrity and availability of computer data and systems.**(Articles 2–6),
- 2) **Computer-related offences.**(Articles 7–8),
- 3) **Content-related offences.** (Article 9),
- 4) **Offences related to infringements of copyright and related rights.** (Article 10).

In terms of general substantive principles, *Attempt and aiding or abetting.* (Article 11) and *Corporate liability* for a criminal offence under the Convention on Cybercrime are further defined.

#### 3.1.2 Council of Europe Additional Protocol No. 189 to the Convention on Cybercrime

The Council of Europe Additional Protocol No. 189 on the Convention on Cybercrime [4], adopted on 28<sup>th</sup> January 2003. [5], defines the range of offences which are not covered by the Convention on Cybercrime. The Convention on Cybercrime does not cover offences related to the dissemination of certain "*harmful material*". [6] The Additional Protocol defines criminal offences which consist primarily in the dissemination of material containing racist, xenophobic or otherwise manifesting racial intolerance. The reason for not including the crimes in question in the Convention on Cybercrime was, in particular, the signing and subsequent acceptance of the Convention on Cybercrime by the USA. [7]

The Additional Protocol consists of a **preamble** and **16 articles**, which are divided into 4 chapters:

##### 1. Common provisions

##### 2. Measures to be taken at the national level



- Article 3 – Dissemination of racist and xenophobic material through computer systems
- Article 4 – Racist and xenophobic motivated threat
- Article 5 – Racist and xenophobic motivated insult
- Article 6 – Denial, gross minimisation, approval or justification of genocide or crimes against humanity

### 3. Relationship between the Convention on Cybercrime and the Additional Protocol

#### 4. Final provisions

The **first chapter** regulates the purpose of the Additional Protocol and defines the term – racist and xenophobic material. According to Article 1 (1) of the Additional Protocol, racist and xenophobic material means *"any written material, image or other expression of ideas or theories which defends, encourages or incites hatred, discrimination or violence against any individual or group of individuals, on the basis of race, colour, gender or national or ethnic origin, as well as religion, if used as an excuse instead of one of these attributes."*

### 3.1.3 EU/EC documents used to harmonise legislation in the fight against cybercrime

In particular, due to the specific nature of cybercrime and the need for effective international cooperation, the EU seeks to approximate the legislation of individual Member States so that this negative phenomenon can be more effectively prosecuted. Framework decisions, directives, and other EU/EC documents are primarily a means of coming into line with the laws of individual EU countries. From the point of view of the fight against cybercrime, the most important documents are the following:

- *Council Directive 91/250/EEC* on the legal protection of computer programs
- *Council Decision 92/242/EEC* on the security of information systems
- *Directive 98/34/EC of the European Parliament and of the Council* on the procedure for the provision of information in the field of technical standards and regulations, as amended by Directive 98/48/EC
- *Directive 2000/31/EC* on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce")
- *Council Framework Decision 2000/375/JHA* on combating child pornography on the Internet
- *Directive 2002/21/EC of the European Parliament and of the Council* on a common regulatory framework for electronic communications networks and services (Framework Directive)
- *Directive 2002/19/EC of the European Parliament and of the Council* on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive)
- *Directive 2002/20/EC of the European Parliament and of the Council* on the authorisation of electronic communications networks and services (Authorisation Directive)
- *Directive 2002/22/EC of the European Parliament and of the Council* on universal service and user rights relating to electronic communications networks and services (Universal Service Directive)
- *Directive 2002/58/EC of the European Parliament and of the Council* concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on the protection of data in electronic communications)
- *Commission Directive 2002/77/EC* on competition in the markets for electronic communications networks and services (Competition Directive)
- *EU Council Framework Decision 2002/584/JHA* on the European arrest warrant and the surrender procedures between Member States
- *Council Framework Decision 2004/68/JHA* on combating the sexual exploitation of children and child pornography
- **Council Framework Decision 2005/222/JHA on attacks against information systems**
- *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – Fight against spam and spyware and malicious software of 15 November 2006*
- *Communication from the Commission to the European Parliament, the Council and the European Committee of the Regions on a general policy on the fight against cybercrime of 22 May 2007*
- *Council Conclusions on a common working strategy and concrete measures to combat cybercrime of 27 November 2008*
- *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on critical information infrastructure protection "Protecting Europe from large-scale cyberattacks and intrusions: enhancing preparedness, security and resilience" of 30 March 2009*
- *Communication from the Commission to the Council and the European Parliament, Tackling crime in the digital age: setting up the European Cybercrime Centre. 2012*
- *Regulation (EU) No 526/2013 of the European Parliament and of the Council on the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 of 21 May 2013*

- *Directive 2013/40/EU of the European Parliament and of the Council on attacks on information systems and replacing Council Framework Decision 2005/222/JHA of 12 August 2013*
- *Regulation (EU) No 513/2014 of the European Parliament and of the Council establishing, as part of the Internal Security Fund, an instrument for financial support for police cooperation, preventing and combating crime and crisis management and repealing Council Decision 2007/125/JHA, of 16 April 2014*
- *Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC of 23 July 2014 (eIDAS, or eIDAS Regulation)*
- *Regulation (EU) 2016/794 of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation (Europol) and repealing and replacing Decision 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, of 11 May 2016*
- *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation)*
- *Directive of the European Parliament and of the Council (EU) 2016/1148, on measures to ensure a high common level of security of networks and information systems in the Union of 6 July 2016 (NIS Directive)*
- *Directive of the European Parliament and of the Council (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA of 17 April 2019*
- *Council Conclusions on a common working strategy and concrete measures to combat cybercrime of 27 November 2008*
- *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection "Protecting Europe from large-scale cyberattacks and intrusions: enhancing preparedness, security and resilience" of 30 March 2009*

### 3.1.4. Legal norms of the Czech Republic

In connection with cybercrime and cybersecurity, it is necessary to mention the legal norms of the Czech Republic, which are directly related to this issue:

- Act No. 40/2009 Sb., Criminal Code
- Act No. 141/1961 Sb., on Criminal Court Proceedings
- Act No. 218/2003 Sb., Act on Juvenile Justice
- Act No. 121/2000 Sb., Copyright Act
- Act No. 127/2005 Sb., on Electronic Communications
- Act No. 480/2004 Sb., on Certain Information Society Services
- Act No. 273/2008 Sb., on the Police of the Czech Republic
- Act No. 89/2012 Sb., Civil Code
- Act No. 110/2019 Sb., on the Processing of Personal Data
- Act No. 14/1993 Sb., on Measures for the Protection of Industrial Property
- Act No. 441/2003 Sb., on Trademarks
- Act No. 527/1990 Sb., on Inventions, Industrial Designs and Improvement Proposals
- Act No. 300/2008 Sb., on Electronic Acts and Authorised Conversion of Documents, as amended
- Act No. 297/2016 Sb., on Services Creating Trust for Electronic Transactions
- Act No. 160/1999 Sb., on Free Access to Information
- Act No. 181/2014 Sb., on Cybersecurity and on Amendments to Related Acts (Cybersecurity Act)

### 3.1.5. Legal norms of Poland

In Polish law, the main regulations regarding cybercrime are:

- Illegal access to a system (hacking) - Art. 267 § 1 and 2 of the Penal Code. This crime is prosecuted at the request of the aggrieved party. They are punishable by a fine, restriction of liberty or imprisonment for up to 2 years.
- Breach of the secret of communication (sniffing) - art. 267 § 3 of the Penal Code. This type of crime consists in obtaining proprietary information, e.g. through sniffers, i.e. programs that intercept data (passwords and user IDs). Such an act is punishable by up to 2 years imprisonment.
- Violation of data integrity (viruses, trojans), 268 of the Penal Code, Art. 268a of the Penal Code. This offence concerns, inter alia, stealing personal data, making them available to third parties without the consent of the owner, as well as use them in an unauthorised way. There are financial sanctions (up to PLN 100,000) for committing these acts.
- Breach of system integrity - Art. 269 of the Penal Code. An example of such a crime are, Ping flood attacks, which consist in overloading the Internet connection. They can, for example, lead to the unavailability of certain services. The Polish legislator provided for a maximum penalty for this act of up to 8 years imprisonment (in the case of a breach of state security).
- Crafting "hacking tools" - Art. 269a of the Penal Code, Art. 269b of the Penal Code. Committing this offence is punishable by a penalty of 3 months to 5 years imprisonment.
- Act of 5 July 2018 on the national cybersecurity system.

### 3.1.6. Legal norms of Portugal

Regarding cybercrime and cybersecurity, in Portugal are in force the following Legal Acts, several of them repeatedly amended:

- Law No. 109/2009, the Cybercrime Law
- Decree-Law No. 48/95, the Criminal Code
- Law No. 103/2015, on the criminal registry of convicted offenders for minors sexual self-determination offences
- Law No. 52/2003, on the fight against terrorism
- Law No 58/2019, on data protection, including related crimes
- Law No. 59/2019, on the processing of personal data for the purpose of preventing, detecting, investigating or prosecuting criminal offences or the execution of criminal sanctions, including related crimes
- Law No. 32/2008, on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks
- Decree-Law No. 131/2014, on the protection and confidentiality of genetic information, human genetic databases for healthcare and health research purposes
- Decree-Law No. 63/85, the Code of Copyright and Related Rights
- Decree-Law No. 252/94, on computer programmes
- Decree-Law No. 110/2018, the Code of Industrial Property
- Decree-Law No. 122/2000, on databases
- Law No. 46/2018, on cyberspace security
- Decree-Law No. 65/2021, regulating Law No. 46/2018
- Decree-Law No. 62/2011, on critical infrastructures
- Law No. 5/2004, on electronic communications
- Law No. 41/2004, on privacy and data protection in electronic communications
- Law No. 26/2016, on the access to administrative information
- Decree-Law No. 7/2004, on information society services
- Decree-Law No. 12/2021, on electronic identification and trust services
- Law No. 7/2007, on the citizen card
- Law No. 37/2014, on digital mobile key
- Decree-Law No. 91/2018, on payment services and electronic money
- Decree-Law No. 69/2014, approving the constitution of the National Cyber Security Centre

### 3.1.7 Cybercrime in a special part of the Criminal Code

From the point of view of cybercrime, the Criminal Code contains special objective elements of criminal offences, which are focused on cybercrime, or some cyberattacks.

Cybercrime is most generally classified in terms of the use of information and communication technologies in criminal offences where these elements are used as a tool to commit a criminal offence and the objective element of the criminal offence includes the use of these means as a characteristic of the objective element, and criminal offences where elements of information and communication technologies are the target of a offender's attack, i.e. they represent an individual object or material object of attack.

The legislator has included in a special part of the Criminal Code a number of objective elements of criminal offences, which either contain features related to information and communication technologies or can be filled with a cyberattack. These offences include:

- Section 180 Illicit Handling of Personal Data
- Section 181 Infringement of the Rights of Another
- Section 182 Breach of Secrecy of Correspondence
- Section 183 Breach of Confidentiality of Files and other Private Documents
- Section 184 Defamation
- Section 191 Distribution of Pornography
- Section 192 Production and Handling of Child Pornography
- Section 193 Abuse of a Child for Production of Pornography
- Section 193b Establishing Illegal Contacts with a Child
- Section 205 Theft
- Section 206 Unauthorised Use of Another's Property
- Section 209 Fraud
- Section 213 Practice of Unfair Games and Wagers
- Section 214 Participation
- Section 216 Money Laundering
- Section 228 Damage to Another's
- Section 230 Unauthorised Access to Computer Systems and Information Media

- Section 231 Obtainment and Possession of Access Device and Computer System Passwords and other such Data
- Section 232 Damage to Computer Systems and Information Media Records and Interference with Computer Equipment out of Negligence
- Section 234 Unauthorised Obtainment, Forgery and Alteration of Means of Payment
- Section 236 Manufacture and Possession of Forgery Equipment
- Section 264 Distortion of Data and Lack of Records of Exporting Goods and Technologies of Dual Use
- Section 268 Infringement of Trademark Rights and Rights to Other Names
- Section 267 Distortion of Data and Lack of Records of Foreign Trade with Military Material
- Section 269 Infringement of Protected Economical Rights
- Section 270 Infringement of Copyright, Rights Related to Copyright and Rights to Databases
- Section 272 Public Menace
- Section 276 Damage and Compromise of Operation of Publicly Beneficial Facility
- Section 287 Propagation of Drug Addiction
- Section 290 Gaining Control over an Aircraft, Civilian Vessels and Fixed Platform
- Section 291 Endangering the Safety of an Aircraft and Civilian Vessel
- Section 311 Terrorist Attack
- Section 316 Espionage
- Section 317 Endangering Classified Information
- Section 345 False Accusation
- Section 348 Forgery and Alteration of Public Documents
- Section 353 Dangerous Threatening
- Section 354 Dangerous Pursuing
- Section 355 Defamation of Nation, Race, Ethnic or other Group of People
- Section 356 Instigation of Hatred towards a Group of People or of the Suppression of their Rights and Freedoms
- Section 357 Disseminating Hoaxes
- Section 361 Participation in Organised Criminal Group
- Section 364 Incitement to Criminal Offence
- Section 365 Approval of Criminal Offence
- Section 400 Genocide
- Section 403 Establishment, Support and Promotion of Movements Aimed at Suppression of Human Rights and Freedoms
- Section 404 Expressing Sympathies for Movements Seeking to Suppress Human Rights and Freedoms
- Section 405 Denial, Contesting, Approval and Justification of Genocide
- Section 407 Incitation of Offensive War

Under the Criminal Code, these cybercrimes can be classified according to many different criteria. One of the most commonly used classifications of cybercrime is the above-mentioned classification into: [\[8\]](#)

a) **criminal offences in the commission of which the means of information and communication technologies are the subject of protection** (i.e. which are the target of a cyberattack):

- Section 182 Breach of Secrecy of Correspondence
- Section 183 Breach of Confidentiality of Files and other Private Documents
- Section 206 Unauthorised Use of Another's Property
- Section 228 Damage to Another's
- Section 230 Unauthorised Access to Computer Systems and Information Media
- Section 232 Damage to Computer Systems and Information Media Records and Interference with Computer Equipment out of Negligence

- Section 234 Unauthorised Obtainment, Forgery and Alteration of Means of Payment
- Section 264 Distortion of Data and Lack of Records of Exporting Goods and Technologies of Dual Use
- Section 267 Distortion of Data and Lack of Records of Foreign Trade with Military Material
- Section 270 Infringement of Copyright, Rights Related to Copyright and Rights to Databases
- Section 290 Gaining Control over an Aircraft, Civilian Vessels and Fixed Platform
- Section 291 Endangering the Safety of an Aircraft and Civilian Vessel
- Section 311 Terrorist Attack
- Section 317 Endangering Classified Information
- b) criminal offences in which the means of information and communication technologies are used to commit a criminal offence:**
- Section 180 Illicit Handling of Personal Data
- Section 181 Infringement of the Rights of Another
- Section 182 Breach of Secrecy of Correspondence
- Section 184 Defamation
- Section 191 Distribution of Pornography
- Section 192 Production and Handling of Child Pornography
- Section 193 Abuse of a Child for Production of Pornography
- Section 193b Establishing Illegal Contacts with a Child
- Section 205 Theft
- Section 209 Fraud
- Section 213 Practice of Unfair Games and Wagers
- Section 214 Participation
- Section 216 Money Laundering
- Section 230 Unauthorised Access to Computer Systems and Information Media
- Section 231 Obtainment and Possession of Access Device and Computer System Passwords and other such Data
- Section 234 Unauthorised Obtainment, Forgery and Alteration of Means of Payment
- Section 236 Manufacture and Possession of Forgery Equipment
- Section 268 Infringement of Trademark Rights and Rights to Other Names
- Section 269 Infringement of Protected Economical Rights
- Section 272 Public Menace
- Section 276 Damage and Compromise of Operation of Publicly Beneficial Facility
- Section 287 Propagation of Drug Addiction
- Section 316 Espionage
- Section 345 False Accusation
- Section 348 Forgery and Alteration of Public Documents
- Section 353 Dangerous Threatening
- Section 354 Dangerous Pursuing
- Section 355 Defamation of Nation, Race, Ethnic or other Group of People
- Section 356 Instigation of Hatred towards a Group of People or of the Suppression of their Rights and Freedoms
- Section 357 Disseminating Hoaxes
- Section 361 Participation in Organised Criminal Group
- Section 364 Incitement to Criminal Offence

- Section 365 Approval of Criminal Offence
- Section 400 Genocide
- Section 403 Establishment, Support and Promotion of Movements Aimed at Suppression of Human Rights and Freedoms
- Section 407 Incitation of Offensive War

In addition to the above provisions of a special part of the Criminal Code, Section 120 of the Criminal Code also applies to cybercrime. It stipulates that *"misleading persons or taking advantage of their misunderstanding may also be done by interfering **with computer information or data**, interfering **with software equipment** of a computer or by performing **another operation on a computer**, interfering with **an electronic or other technical device**, including the interference with **objects designated to control such a device**, or by using such an operation or interference performed by another person."*

[1] A list of states that have signed and ratified the Convention on Cybercrime can be found at:

[https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p\\_auth=F6wSLE5D](https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=F6wSLE5D).

[2] This obligation is set out in Articles 14–21 of the Convention on Cybercrime.

[3] The full text of the Convention can be found at: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>

[4] *ETS No. 189 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*. [online]. [cit.20.8.2016]. Available from: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168008160f>

[5] A list of states that have signed and ratified the Additional protocol can be found at:

[https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p\\_auth=F6wSLE5D](https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=F6wSLE5D)

[6] With the exception of child pornography, which is directly contained in Article 9 of the Convention on Cybercrime.

[7] It is precisely the issue of racism and xenophobia that is a topic in the "grey zone" in the USA, as some statements can be considered a crime and others cannot. For example, not all manifestations of racism are considered a crime in the **USA**, see the **First Amendment to the U.S. Constitution – the Congress will not pass any law that disregards freedom of religion or prohibits free exercise (worship), or curtails freedom of speech or press, or the right of people to peacefully gather and petition the government with a view to redressing wrongs. In order to be an infringement or a criminal offence, the reality of the threat must be proved. Otherwise, it would be a violation of the first amendment.** In contrast, expressions of racism in **France** or **Germany**, as well as in the **Czech Republic**, are considered a crime.

[8] Due to the diction of their objective elements, some criminal offences can be classified into both categories (these provisions protect the means of information and communication technologies, but at the same time contain signs of misuse of these technologies).

## 3.2. Substantive aspects of cybercrime in Poland

The legislator has included in the Criminal Code a number of objective elements of criminal offences, which either contain features related to information and communication technologies or can be satisfied by a cyberattack. These offences include:

- Art. 126a. Public provocation to commit a prohibited act
- Art. 130. Espionage
- Art. 132. Intelligence disinformation
- Art. 133. Insulting the Nation or the Republic of Poland
- Art. 135. Assault or insult upon the President of the Republic of Poland
- Art. 136. Active assault or insult of a representative of a foreign state
- Art. 137. Public insult of a sign or symbol of the State
- Art. 151. Aiming to commit suicide and giving assistance
- Art. 165. Causing public danger
- Art. 190. Penal threat
- Art. 190a. Stalking
- Art. 191. Forcing a specific conduct, abandonment or suppression
- Art. 191a. Recording the image of a naked person
- Art. 196. Offence against religious feelings of others
- Art. 200a. Electronic contact with a minor for paedophilic purposes
- Article 200b. Public promotion of paedophilic content
- Art. 202. Presentation and distribution of pornography
- Art. 212. Defamation
- Art. 216. Defamation of a person
- Art. 224a. False report of a threat
- Art. 226. Insulting a public official or a constitutional organ of the Republic of Poland
- Art. 227. Misappropriation of the function of a public official
- Art. 228. Bribery of a public functionary
- Art. 229. Bribery
- Article 230. Passive paid patronage
- Article 230a. Active paid patronage
- Article 232. exerting influence on the activities of the court
- Art. 234. False accusation
- Article 235. creation of false evidence
- Art. 236. Withholding evidence of the suspect's innocence
- Art. 238. False report of an offence
- Art. 239. Supporting and abetting
- Art. 240. Criminal failure to report a criminal act
- Art. 241. Unlawful dissemination of the news from the pre-trial proceedings or trial
- Art. 244. Failure to comply with the penal measures ordered by the court
- Article 245. Using violence or threats to influence a participant in the proceedings
- Article 246. Extortion by a public official to give testimony, explanations, information or a statement

- Article 250. Unlawful exertion of influence on a person entitled to vote
- Article 251 Breach of the secrecy of the ballot
- Article 255 Public incitement to commit or praise of a transgression or fiscal offence
- Article 255a. Dissemination of content facilitating the commission of a terrorist offence
- Article 256 Propagation of fascism or another totalitarian regime
- Article 257. Racism
- Art. 265 Disclosure or use of classified information with the clause "secret" or "top secret"
- Art. 266. Disclosure or use of information obtained in connection with the exercise of an official function or activity
- Art. 267 Obtaining information unlawfully
- Article 268 Obstructing the authorised person from learning the information
- Article 268a. Destroying, damaging, deleting, altering or obstructing access to computer data
- Article 269 Destroying, damaging, deleting or altering sensitive computer data
- Article 269a. Interference with operation of an IT system, data communication system or network
- Article 269b. Unlawful production, acquisition, disposal or provision of computer programmes
- Art. 270. Falsifying a document and using it as authentic
- Art. 270a. Falsifying an invoice and using it for authenticity
- Art. 271. Misrepresentation
- Art. 271a. Misrepresentation on an invoice
- Art. 272. Fraudulent use of false statements in a document
- Art. 273. Using a document that is false Article 275.
- Art. 275. Using another person's identity document
- Art. 276. Destroying or concealing a document without the right to dispose of it
- Art. 277a. Falsifying an invoice or using a falsified invoice with the amount stating property of great value
- Art. 278. Theft
- Art. 282. Robbery
- Art. 284. Misappropriation
- Art. 285. Activation of telephone impulses on someone else's account
- Article 286. Fraud
- Art. 287. Computer fraud
- Article 291. Intentional receiving
- Article 292. Unintentional receiving
- Article 293. Computerised taking of property
- Article 296. Causing damage in business dealings
- Article 296a. Bribery in a managerial position
- Art. 297. Extortion of credit
- Art. 298. Extortion of compensation
- Article 299. Money laundering
- Article 300. Hindering satisfaction of the creditor
- Article 303. Failure to keep or false keeping of business records
- Article 304. Exploitation of the contracting party
- Article 305. Interference with public tender



- Art. 306. Removing, counterfeiting or altering identification marks
- Article 310. Falsification of money, means of payment or securities
- Article 311. Falsification of information in securities trading
- Article 312. Circulating counterfeited or forged money, means of payment or payment documents
- Article 313. Falsification of official securities marks
- Article 314. Falsification of official marks with a view to their use in business transactions
- Art. 346. Violence or unlawful threat by a soldier against his superior
- Art. 347. Insult of a superior by a soldier

### 3.3. Substantive aspects of cybercrime in Portugal

The main feature of the Sources regarding cybercrime in the Portuguese Legal System is their dispersion. Even being in place a *Cybercrime Law*, following the Budapest Convention and implementing Council Framework Decision 2005/222/JHA, offenses specifically implying the use of ICT systems were allocated to several other acts, including the *Criminal Code*. Besides, since 1991, crimes related to personal data protection are considered as different from cybercrimes in general, almost with parallel typicalities.

Thus, according to the Portuguese Legal System, cybercrimes can be classified according to many different criteria. One of the most commonly used classifications of cybercrime is the above-mentioned classification into:

**a) criminal offences in the commission of which the means of information and communication technologies are the subject of protection:**

- Illegal access (Art. 6 of Cybercrime Law)
- Computer sabotage [Illegal interference] (Art. 5 of Cybercrime Law)
- Illegal interception (Art. 7 of Cybercrime Law)
- Damage to computer programmes or other computer data [Data interference] (Art. 4 of Cybercrime Law)
- Misuse of devices (Arts. 4(3), 5(2), 6(2) and 7(3) of Cybercrime Law)
- Illegal reproduction of protected computer programme (Art. 8 of Cybercrime Law)
- Illegal reproduction or communication of a copyright protected database (Art. 11 of Decree-Law No. 122/2000)
- Removal or alteration of any electronic rights-management information (Arts. 217 to 219 and 224-224 of the Code of Copyright and Related Rights)
- Breach of the exclusive rights on topographies of semiconductor products (Art. 318 of the Industrial Property Code)
- Breach of correspondence or telecommunications (Art. 194 of the Criminal Code)

**b) criminal offences in which the means of information and communication technologies are used to commit a criminal offence:**

- Inappropriate access to personal data (Art. 47 of Law No. 58/2019)
- Incompatible use of personal data with the purpose of processing (Art. 46 of Law No. 58/2019)
- Misappropriation of personal data (Art. 48 of Law No. 58/2019)
- Tampering or destruction of personal data (Art. 49 of Law No. 58/2009)
- Entering of false personal data (Art. 50 of Law No. 58/2009)
- Breach of secrecy related to personal data (Art. 51 of Law No. 58/2009)
- Disobedience [to the National Commission for the Protection of Data] (Art. 52 of Law No. 58/2009)
- Illegal processing of sensitive personal data (Art. 193 of the Criminal Code)
- Aggravated breach of privacy (Arts. 191(1)(b) and 197(b) of the Criminal Code)
- Inappropriate access to personal data in criminal justice (Art. 53 of Law No. 59/2019)
- Misappropriation of personal data in criminal justice (Art. 54 of Law No. 59/2019)
- Incompatible use of personal data with the purpose of processing in criminal justice (Art. 55 of Law No. 59/2019)
- Illegal Interconnection of personal data in criminal justice (Art. 56 of Law No. 59/2019)
- Qualified disobedience [to the National Commission for the Protection of Data] in criminal justice (Art. 57 of Law No. 59/2019)
- Entering of false personal data in criminal justice (Art. 58 of Law No. 59/2019)
- Revenge pornography related to domestic violence (Art. 152(2)(b) of the Criminal Code)
- Offences related to child pornography (Art. 176 of the Criminal Code)
- Solicitation of children for sexual purposes (Art. 176-A of the Criminal Code)
- Computer-related forgery (Art. 3 of Cybercrime Law)
- Counterfeiting of cards and other non-cash means of payment (Art. 3-A of Cybercrime Law)
- Computer [and telecommunications]-related fraud (Art. 221 of the Criminal Code)
- Use of counterfeited cards and other non-cash means of payment (Art. 3-B of Cybercrime Law)

- Acquisition of counterfeited cards and other non-cash means of payment (Art. 3-C of Cybercrime Law)
- Misuse of devices related to the Counterfeiting of cards and other non-cash means of payment (Art. 3-D of Cybercrime Law)
- Acquisition of of counterfeited cards and other non-cash means of payment obtained by computer crimes (Art. 3-E of Cybercrime Law)

With indirect connections, these felonies might also be mentioned:

- Sexual Harassment (Art. 170 of the Criminal Code)
- Insult (Art. 181 of the Criminal Code)
- Defamation (Art. 180 of the Criminal Code)
- Breach of privacy (Art. 192 of the Criminal Code)
- Discrimination and incitement to hate and violence (Art. 240 of the Criminal Code)
- Counterfeiting of copyrighted works (Art. 196 of the Code of Copyright and Related Rights)
- Copying, distribution and selling of copyrighted works (Art. 195 of the Code of Copyright and Related Rights)

## 4. Manifestations of cybercrime

Cybercrime is typically manifested through cyberattacks, but purely non-technical aspects must be used to successfully carry out a number of attacks.

Certain illegal conduct in cyberspace or cybercrime-related conduct can be classified under the relevant provisions of the current Criminal Code, but there are certain types of conduct that may be significantly more complicated, or even impossible, to criminalise (in many cases it is rather immoral).

Very often cybercrime is considered a new type of crime. However, a significant part of cybercrime uses or transfers notorious types of illegal conduct (such as fraud, copyright infringement, theft, bullying, etc.) to the digital environment, where they can be committed "better, faster and more effectively" than in the real world. Among the purely cyberattacks, the following, for example, could be included hacking, DoS and DDoS attacks, botnets, etc.

It is characteristic of the virtual world that most users have an incomprehensible, almost limitless trust in it. At the same time, it must be stated that the virtual world is becoming more and more important for us. Personally, I feel that when using the services provided on the Internet, many people stop thinking about possible risks or threats. They are primarily captivated by the seemingly endless possibilities of "new technologies"; how else is it possible to explain the absence of basic defence principles and mechanisms in the virtual world, when in the real world we would behave completely differently. Sometimes, the behaviour of users in cyberspace remind me of the "Strange Case of Dr. Jekyll and Mr. Hyde" by Robert Louise Stevenson (1886). Seemingly decent people in the real world act without any legal or moral restraints in the "pseudo-anonymous" environment of cyberspace. So, for example, it is possible to come across a case of a judge downloading "child pornography"[\[1\]](#), users who have never stolen anything in the real world but have no problem stealing in the virtual world[\[2\]](#), or violating other rights protected by the law of a country.

A number of leading experts have commented on the predictions of the development of cybercrime in the past, of which I would like to quote Schneier in particular, who predicted in 2002 that the next major security trend on the Internet would be crime. *"Not cases of viruses, Trojans and DDoS attacks for fun or the opportunity to show off your skills. It will be a real crime. On the Internet. Criminals tend to lag behind technology development by five or ten years, but eventually realise their potential. Just as Willie Sutton began robbing banks "because there was money," so modern criminals will begin to attack via computer networks. More and more values (funds) are online than in real money."*[\[3\]](#)

In 2007, the FBI introduced statistics that compared a common "bank robbery" with conduct that is a phishing attack.[\[4\]](#)

Parameter	Average armed robbery	Average cyberattack
<b>Risk</b>	The offender risks being injured or killed.	No risk of physical harm
<b>Profit</b>	On average, USD 3–5 thousand.	On average, USD 50–500 thousand.
<b>Probability of catching</b>	50–60% of attackers caught.	About 10% of attackers caught.
<b>Probability of conviction</b>	95% of caught attackers convicted.	Of the caught attackers, only 15% of the attackers will go to trial and only 50% will be convicted.
<b>Punishment</b>	On average 5–6 years, if the offender did not injure anyone during the robbery.	On average 2–4 years.

In 2012, in relation to information and communication technologies, Goodman stated that *"an individual's ability to influence masses, due to these technologies, is growing exponentially. It is growing exponentially for both good and bad purposes"*. He clearly presents this growth in the development of the crime of robbery, for which a knife or pistol was originally enough in the past, and robbery essentially meant an act between individuals or small groups. *"A major 'innovation' took place at the time of a robbery of an entire train carrying 200 people."* The Internet allows for an even greater scale of an attack by one person. The robbery of a large number of users is clearly demonstrated by the case of the Sony Playstation with approximately 100 million injured people. *"When in the history of mankind could an individual rob 100 million people? But it's not just about thefts..."*[\[5\]](#)

In the same year, Robert S. Mueller, FBI Director, gave a speech in the RSA Cyber Security Conference (San Francisco, CA), where he stated, inter alia: *"I believe there are only two types of companies: those that have been hacked and those that will be hacked. And even they are converging into one category: companies that have been hacked and will be hacked again."*[\[6\]](#)

Currently, there is an increasing and massive interconnection of various computer systems into cyberspace, which practically generates a direct relationship consisting of the following statement: *"the more devices connected, the greater their vulnerability and the greater the number of attacks."* One of the graphical representations of the ongoing attacks can be found at: <http://map.norsecorp.com/#/>; <https://cybermap.kaspersky.com/>; <https://map.lookingglasscyber.com/> etc.

We believe that there is no doubt that cybercrime is on the rise, and it is a global problem. Various statistics show partially different damages caused by cybercrime, but this does not change the fact that they all include primary damages (e.g. malfunction of a computer system, its parts, services offered, infrastructure failure, etc.) and secondary damage (e.g. system recovery, data recovery, reconnection of end users, etc.). Europol reports in its 2014 report[\[7\]](#) that cybercrime costs the global economy around USD 300 billion a year. The community of attackers has changed considerably since the mass expansion of the Internet. Primarily, it means that there are no longer individuals who have committed offences for fun or circumventing barriers. At present, these are usually professionals who do their job in order to profit and are often involved in organised groups.

This shift is understandable and inextricably linked to three aspects:

- 1) **Dependence of the society on the Internet** (or offered services, technologies, etc.),
- 2) **Cybercrime has become a lucrative global business** [the first cyber attacks have already shown the potential for profit, either directly (by drawing funds) or indirectly (e.g. by paying for damage to another person's service)].
- 3) **Minimum literacy of users** who use information and communication technologies (the user is a typical example of the weakest link in the chain).

With the development of all kinds of services based on the principle of as-a-service[8], a number of platforms (typically underground, darknet forums) have emerged in the cybercrime environment, where services are offered that can be described as **crime-as-a-service** (cybercrime- as-a-service). Thus, a "malware or underground economy" emerges that provides almost any user with the means to commit cybercrime. The following services are offered as standard within the service collectively referred to as crime-as-a-service:

- *Research-as-a-service*,[9]
- *Crimeware-as-a-service*,[10]
- *Infrastructure-as-a-service*,[11]
- *Hacking-as-a-service*, [12]
- *Data-as-a-service*,[13]
- *Spam-as-a-service*,[14]
- *Ransomware-as-a-service* etc.

The list of individual services is not exhaustive, and it can be stated that crime-as-a-service includes the possibility to order any conceivable service or commodity that can be used or obtained in cyberspace. The rise of these negative activities is directly linked to the phenomenon of the Internet of Things (IoT), which connects devices (computer systems) with the Internet, and thus poses another significant threat, which lies primarily in disregarding one of the basic principles of security.

Many manufacturers or distributors of computer systems that can be classified as IoT do not address the issue of security (their goal being to bring to market and sell as many devices that can be described as a computer system as possible), which attackers use.

The costs associated with security developments are usually the most costly part of development, but this is an area that needs to be addressed in view of the threats already known. These include, for example: an unsecured communication channel of a pacemaker[15]; a remote- controlled car or aircraft[16]; smart household or its components (refrigerator, boiler, security system, television, etc.), which can be controlled remotely[17], etc.

*"How will the world turn out when we are already using 6.4 billion IoT devices **this year**? Over the next four years, it should be 20.8 billion devices. In addition, many of these devices will have a significantly longer lifespan than the normal life cycle of mobile phones, tablets or laptops. How will a car manufacturer be able to protect the security of the 2020 model ten years later? Or a refrigerator that can stand at your home for fifteen years or more? How long did it take Microsoft to learn how to update its own operating system?"*[18]

Schneier states that when it comes to data, attackers can do essentially three basic things with them: steal them (violating the principle of **Confidentiality**), alter them (violating the principle of **Integrity**) or prevent owners from accessing them (violating the principle of **Availability**). Schneier states that with the advent of IoT, the last two types of attacks will become extremely effective.[19]

In the following section, I will introduce some of the attacks that occur in the cyberspace environment. It is not possible to define all attacks, either because of the scope of this publication or because of the impossibility of describing all possible alternative acts subsumable under the term cybercrime. If possible, the specific criminal law qualification of such conduct will be stated for a specific manifestation of cybercrime.

---

[1] Judge, 69, who downloaded child porn facing 'catastrophic humiliation'. [online]. [cit.1.9.2009]. Available from: <http://news.sciencemag.org/social-sciences/2015/02/facebook-will-soon-be-able-id-you-any-photo>

[2] HILL, Kashmir. *These two Diablo III players stole virtual armor and gold — and got prosecuted IRL*. [online]. [cit.10.8.2015]. Available from: <http://fusion.net/story/137157/two-diablo-iii-players-now-have-criminal-records-for-stealing-virtual-items-from-other-players/>

[3] For more details see SCHNEIER, Bruce. *Crime: The Internet's Next Big Thing*. [online]. [cit.6.11.2007]. Available from: <https://www.schneier.com/crypto-gram/archives/2002/1215.html>

[4] JIROVSKÝ, Václav. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Prague: Grada, 2007, p. 30

[5] For more details see GOODMAN, Marc. *A vision of crimes in the future*. [online]. [cit.13.11.2014]. Available from: [https://www.ted.com/talks/marc\\_goodman\\_a\\_vision\\_of\\_crimes\\_in\\_the\\_future#t-456071](https://www.ted.com/talks/marc_goodman_a_vision_of_crimes_in_the_future#t-456071)

[6] MUELLER, Robert. [online]. [cit.3.4.2013]. Available from: <https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies>

[7] See *The Internet Organised Crime Threat Assessment (iOCTA) 2014*. [online]. [cit.10.8.2015]. Available from: <https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta>

[8] It is the provision of services typically associated with a cloud solution. Examples are: infrastructure-as-a-service; platform-as-a-service; Service-as-a-service; Security-as-a-service etc.

[9] Under this service, it is possible to imagine activities that consist in detecting various, as yet unknown vulnerabilities of the target computer system or software. (These vulnerabilities are known as zero-day vulnerabilities.)

The actual activity within research-as-a-service does not necessarily have to be in its nature a criminal or illegal act. Vulnerability and error detection is performed by a number of IT security experts (e.g. penetration testing, etc.). Typically, these services are provided on the basis of contractual terms between the testee and the tester, or using some of the circumstances precluding illegality.

[10] The crimeware-as-a-service offers a wide range of activities from the simple sale of malware, through its "customisation", as well as the delivery of exploits (vulnerabilities), etc.

[11] Infrastructure-as-a-service then offers the offer of physical or virtual computer systems (botnets, hosting services, network leases, etc.).

[12] This service can include a simple breaking of access data to e-mail, social network account, etc., up to professional and sophisticated attacks on a selected victim. This area can then include, for example, the execution of DoS and DDoS attacks.

[13] The data-as-a-service offers the most sought-after commodity, which is data. Specifically, these are, for example: access data (name and password) to various accounts, credit cards, bank accounts, stolen credit cards, but also information about persons (residence, date of birth, telephone numbers, e-mails, etc.).

[14] The name implies that it is possible to order and pay for a spam campaign.

[15] Cf. TAYLOR, Harriet. *How the "Internet of Things" could be fatal*. [online]. [cit.17.6.2016]. Available from: <http://www.cnn.com/2016/03/04/how-the-internet-of-things-could-be-fatal.html>

[16] For more details see REENBERG, Andy. *Hackers remotely kill a Jeep on the highway – with me in it*. [online]. [cit.4.5.2016]. Available from: <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>

In the Czech version available, for example, from: [http://auto.idnes.cz/hackeri-unesli-jeep-dalkove-ovladani-auta-f11-/automoto.aspx?c=A150723\\_135910\\_automoto\\_fdv](http://auto.idnes.cz/hackeri-unesli-jeep-dalkove-ovladani-auta-f11-/automoto.aspx?c=A150723_135910_automoto_fdv)

For more details see ZETTER, Kim. *Is It Possible for Passengers to Hack Commercial Aircraft?* [online]. [cit.5.5.2016]. Available from: <https://www.wired.com/2015/05/possible-passengers-hack-commercial-aircraft/>

[17] It is thus possible, for example, to circumvent household security; increase the temperature with the remote-controlled thermostat and cause damage to another person; order a meaningless amount of food through a "smart" refrigerator, etc.

[18] DOČEKAL, Daniel. *Bruce Schneier: Internet věci přinese útoky, které si neumíme představit*. [online]. [cit.10.8.2016]. Available from: <http://www.lupa.cz/clanky/bruce-schneier-internet-veci-prinese-utoky-ktere-si-neumime-predstavit/>

[19] SCHNEIER, Bruce. *The Internet of Things Will Turn Large-Scale Hacks into a Real World Disasters*. [online]. [cit.10.8.2016]. Available from: <https://motherboard.vice.com/read/the-internet-of-things-will-cause-the-first-ever-large-scale-internet-disaster>

## 4.1. Social Engineering

Social engineering cannot be considered directly to apply across the board to a cyberattack, but it is a prerequisite for a number of cyberattacks to be successful.

If we wanted to define the concept of social engineering, it could be said that it is about influencing, persuading or manipulating people in order to force them to take a certain action or to obtain information from them that they would not otherwise provide. The purpose is to give a victim such an impression that the situation in which they are is different from what it really is. To put it more simply, it is the "art of deception", with Mitnick distinguishing two specialisations in the profession of artist-manipulator. *"The one who makes money from people is an ordinary fraudster, while the one who uses manipulation and persuasion against companies – usually with the intention of obtaining information – is a social engineer."*[1]

I am convinced that this Mitnick's claim from 2003 would not stand up in today's digital world as many attackers use social engineering techniques to obtain information or data and use it, for example, in crime-as-a-service. Furthermore, these techniques are used not only for companies but also for individuals. An actual attack does not have to take the form of fraud, but subsequently this information can be sold or misused for a more serious attack.

The main idea of social engineering is not to use various purely technical approaches or tools, for example to break a password, when it is much easier to mislead a victim, who can voluntarily reveal the password. The weakest link in the security system is and always will be a person (the user). Since there cannot be a computer system in the world that is not dependent on humans, at least at some stage (whether it is the operation, setup or maintenance of a computer system), the easiest way is to obtain the necessary information from people.

It is the simplicity of an attack aimed at the weakest link in the whole system that usually makes it the most effective form. Social engineering came to the fore with the case of Mitnick[2], who is considered by many to be a hacker, but he actually considers himself to be a social engineer. In his books[3], Mitnick shows how easy it is to obtain information that is sensitive and poses a security risk to individuals and organisations. At a hearing before U.S. Senate Committee on Governmental Affairs[4], in which Mitnick testified about obtaining passwords and sensitive information about the computer systems of the companies he hacked into, Mitnick said: *"I introduced myself as someone else and simply asked for them."*

For social engineering, one of the key factors is to obtain as much information as possible about the target of the attack (whether a computer system, a legal entity or a natural person). There is often a long-term effect on a key person and building "trust" between an attacker and a victim before an attack, while the attacker typically exploits human carelessness, trust, willingness to help others, laziness, weakness, fear (e.g. so that the person does not get into trouble), irresponsibility, stupidity, etc.

The above human characteristics greatly help an attacker to carry out his attack. Ask yourself how much do you verify your counterparty, for example when making a phone call or communicating via ICT? How much do you check the storage media (USB disks, memory cards, etc.) that you received as a gift for the presentation event?

Especially in the field of ICT, it is possible to observe increasingly more sophisticated and elaborate attacks [e.g. well-prepared fraudulent e-mails, real institutions (used as an alleged sender), redirection to fraudulent sites or installation of malware contained in a document attachment or on a storage medium, etc.].

Social engineering attacks are usually conducted in three ways, and these methods are combined with each other:

1. **Collection of freely (publicly) available data** on a target of an attack
2. **Physical attack** (for example, an attacker pretends to be a service agency employee – such as a printer service, maintenance worker, etc.), in which the attacker tries to obtain as much information "from inside" the company, or sensitive information about individual employees (including e.g. searching garbage, etc.)

### 3. **Psychological attack**

The most common methods of social engineering attacks include:

1. **Fraudulent e-mail or fake website**
2. **Telephone call**
3. **"Face to face" attack**
4. **Dumpster diving** as well as "data straining"
5. **Searching websites, social networks, etc.** (This is an easily accessible open source of data for attackers of social engineering, which helps to identify or verify information about a potential target.) **Public information available online** (e.g. CVs, theses, papers, proposals, etc. published on the Internet). **Annual reports and other publicly available information about a company**
6. **Delivery of advertising or other materials on CD, DVD or other storage media**
7. **Leaving a storage medium** (USB, etc.) **in an area of interest** (such as company, employee's house, etc., such medium then typically contains malware)
8. **Offer to try a service online** (e.g. offer of a cloud storage, or an interesting service for free, etc.)
9. **Delivery or finding of equipment** (computer system)
10. **Fake service technician**
11. **Others**

As for targets of social engineering attacks within an organisation, possible targets may be, for example:

- management position,
- IT department,
- helpdesk workers,
- receptionists (secretaries),
- security staff,
- building management,
- cleaning etc.

A social engineer is able due to his capacity to manipulate people, however, simple manipulation is not enough in some cases and it is necessary to link this information with technical knowledge in the field of ICT.

At the end of this chapter, I give an example in which Mitnick demonstrates the connection between social techniques and ICT knowledge:[\[5\]](#)

A young attacker I'll call Ivan Peters set out to retrieve the source code for a new electronic game. He had no trouble getting into the company's wide area network because a hacker buddy of his had already compromised one of the company's web servers. After finding an unpatched vulnerability in the web server software, his buddy had just about fallen out of his chair. When he realised the system had been set up as a *dual-homed* host, which meant he had an entry point into the internal network.

But once Ivan was connected, he then faced a challenge that was like being inside the Louvre and hoping to find the Mona Lisa. Without a floor plan, you could wander for weeks. The company was global, with hundreds of offices and thousands of computer servers, and they didn't exactly provide an index of development systems or the services of a tour guide to steer him to the right one. Instead of using a technical approach to finding out what server he needed to target, Ivan used a social engineering approach. He placed phone calls based on methods similar to those described elsewhere in this book. First calling IT technical support, he claimed to be a company employee having an interface issue on a product his group was designing, and asked for the phone number of the project leader for the gaming development team. Then he called the name he'd been given, posing as a guy from IT. "*Later tonight,*" he said, "*we're swapping out a router and need to make sure the people on your team don't lose connectivity to your server. So we need to know which servers your team uses.*" The network was being upgraded all the time. And giving the name of the server wouldn't hurt anything anyway, now would it? Since it was password-protected, just having the name couldn't help anybody break in. So the guy gave the attacker the server name. Didn't even bother to call the man back to verify his story, or write down his name and phone number. He just gave the name of the servers, ATM5 and ATM6.

At this point, Ivan switched to a technical approach to get the authentication information. The first step with most technical attacks on systems that provide remote access capability is to identify an account with a weak password, which provides an initial entry point into the system. When an attacker attempts to use hacking tools for remotely identifying passwords, the effort may require him to stay connected to the company's network for hours at a time.

Clearly he does this at his peril: the longer he stays connected, the greater the risk of detection and getting caught. As a preliminary step, Ivan would do an enumeration, which reveals details about a target system. Once again the Internet conveniently provides software for the purpose (<http://mtslenth.0catch.com>). Ivan found several publicly available hacking tools on the web that automated the enumeration process, avoiding the need to do it by hand, which would take longer and thus run a higher risk. Knowing that the organisation mostly deployed Windows-based servers, he downloaded a copy of NBTEnum, a NetBIOS (basic input/output system) enumeration utility[\[6\]](#). He entered the IP (Internet protocol) address of the ATM5 server, and started running the program. The enumeration tool was able to identify several accounts that existed on the server.

Once the existing accounts had been identified, the same enumeration tool had the ability to launch a dictionary attack against the computer system. A dictionary attack is something that many computer security folks and intruders are intimately familiar with, but that most other people will probably be shocked to learn is possible. Such an attack is aimed at uncovering the password of each user on the system by using commonly used words. We're all lazy about some things, but it never ceases to amaze me that when people choose their passwords, their creativity and imagination seem to disappear. Most of us want a password that gives us protection but that is at the same time easy to remember, which usually means something closely connected to us. Our initials, middle name, nickname, spouse's name, favorite song, movie, or brew, for example. The name of the street we live on or the town we live in, the kind of car we drive, the beachfront village we like to stay at in Hawaii, or that favorite stream with the best trout fishing around. Recognise the pattern here? These are mostly personal names, place names, or dictionary words. A dictionary attack runs through common words at a very rapid pace, trying each as a password on one or more user accounts.

Ivan ran the dictionary attack in three phases. For the first, he used a simple list of some 800 of the most common passwords. The list includes *secret*, *work*, and *password*. Also the program permuted the dictionary words to try each word with an appended digit, or appending the number of the current month. The program tried each attempt against all of the user accounts that had been identified. No luck. For the next attempt, Ivan went to Google's search engine and typed "*wordlists dictionaries*" and found thousands of sites with extensive wordlists and dictionaries for English and several foreign languages. He downloaded an entire electronic English dictionary. He then enhanced this by downloading a number of word lists that he found with Google. Ivan chose the site at [www.outpost9.com/files/Wordlists.html](http://www.outpost9.com/files/Wordlists.html). This site allowed him to download (all of this for free) a selection of files including family names, given names, congressional names and words, actor's names, and words and names from the Bible. Another of the many sites offering word lists is actually provided through Oxford University, at <ftp://ftp.ox.ac.uk/pub/wordlists>. Other sites offer lists with the names of cartoon characters, words used in Shakespeare, in the Odyssey, Tolkien, and the Star Trek series, as well as in science and religion, and on and on. (One on-line company sells a list containing 4.4 million words and names for only \$20.) The attack program can be set to test the anagrams of the dictionary words, as well – another favorite method that many computer users think increases their safety.

Once Ivan had decided which wordlist to use, and started the attack, the software ran on autopilot. He was able to turn his attention to other things. And here's the incredible part: You would think such an attack would allow the hacker to take a Rip van Winkle snooze and the software would still have made little progress when he awoke. In fact, depending on the platform being attacked, the security configuration of the system, and network connectivity, the complete English vocabulary can, incredibly, be tried in less than thirty minutes! While this attack was running, Ivan started another computer running a similar attack on the other server used by the development group, ATM6. Twenty minutes later, the attack software had done what most unsuspecting users like to think is impossible: It had broken a password, revealing that one of the users had chosen the password "*Frodo*," one of the Hobbits in the book *The Lord of the Rings*. With this password in hand, Ivan was able to connect to the ATM6 server using the user's account. There was good news



and bad news for our attacker. The good news was that the account he cracked had administrator privileges, which would be essential for the next step. The bad news was that the source code for the game was not anywhere to be found. It must be, after all, on the other machine, the ATM5, which he already knew was resistant to a dictionary attack. But Ivan wasn't giving up just yet; he still had a few more tricks up his sleeve. On some Windows and UNIX operating systems, password hashes (encrypted passwords) are openly available to anyone who has access to the computer they're stored on. The reasoning is that the encrypted passwords cannot be broken and therefore do not need to be protected. The theory is wrong. Using another tool called *pwdump3*, also available on the Internet, he was able to extract the password hashes from the ATM6 machine and download them. A typical file of password hashes looks like this:

Administrator: 500:95E4321A38AD8D6AB75E0C8D76954A50:

2E48927AQB04F3BFB341E266D6L

akasper:1110:5A8D7E9E3C3954F642C5C736306CBFEF:393CE7F90A8357F157873D72D

digger:1111:5D15COD58D0216C525AD3B83FA6627C7:17AD564144308B42B8403D01AE256

555

ellgan:1112:2017DA45D801383EFF17365FAF1FFE89:07AEC950C22CBB9C2C734EB89j1

tafeeck:1115:9F5890B3FECCAB7EAAD3B435B51404EE:1F0115A728447212FC05E1D208203

35

vkantar;1116:81A6A5D035596E7DAAD3B435B51404EE:B933D36DD12258946FCC7BD153F1

CD6

vwallwick:1119:25904EC665BA30F44494F42E1054F192:15B2B7953FB632907455D2706A432

mmcdonald: 1121:

A4AED098D29A3217AAD3B435B51404EE:40670F936B79C2ED522F5ECA939c

kworkman:1141:C5C598AF45768635AAD3B435B51404EE:DEC8E827A121273EF084CDBF5F

D192

With the hashes now downloaded to his computer, Ivan used another tool that performed a different flavour of password attack known as *brute force*.<sup>[2]</sup> This kind of attack tries every combination of alphanumeric characters and most special symbols.

Ivan used a software utility called *L0phtcrack3* (pronounced loft-crack; available at [www.atstake.com](http://www.atstake.com); another source for some excellent password recovery tools is [www.elcomsoft.com](http://www.elcomsoft.com)). System administrators use L0pht-crack3 to audit "weak" passwords; attackers use it to crack passwords. The brute force feature in LC3 tries passwords with combinations of letters, numerals, and most symbols including @#\$\$%^&. It systematically tries every possible combination of most characters. (Note, however, that if nonprintable characters are used, LC3 will be unable to discover the password.) The program has a nearly unbelievable speed, which can reach to as high as 2.8 million attempts a second on a machine with a 1 GHz processor. Even with this speed, and if the system administrator has configured the Windows operating system properly (disabling the use of LANMAN hashes), breaking a password can still take an excessive amount of time. For that reason the attacker often downloads the hashes and runs the attack on his or another machine, rather than staying online on the target company's network and risking detection. For Ivan, the wait was not that long.

Several hours later the program presented him with passwords for every one of the development team members. But these were the passwords for users on the ATM6 machine, and he already knew the game source code he was after was not on this server. What now? He still had not been able to get a password for an account on the ATM5 machine. Using his hacker mindset and understanding the poor security habits of typical users, he figured one of the team members might have chosen the same password for both machines. In fact, that's exactly what he found. One of the team members was using the password "gamers" on both ATM5 and ATM6. The door had swung wide open for Ivan to hunt around until he found the programs he was after.

Once he located the source-code tree and gleefully downloaded it, he took one further step typical of system crackers: He changed the password of a dormant account that had administrator rights, just in case he wanted to get an updated version of the software at some time in the future.

To reduce the risks posed by social engineering, it is necessary to raise awareness of possible threats not only within the organisation, but within society as a whole. As I mentioned earlier, social engineering helps to carry out an attack, and it is entirely up to the attacker to determine who will be his target. It is much easier for an attacker to focus his attack on the masses of inexperienced and ignorant people than on a relatively well-protected company.

---

[1] MITNICK, Kevin D. and William L. SIMON. *The Art of Deception (Uměniklamu)*. Gliwice: Helion, 2003. ISBN 83-7361-210-6. p. 6

[2] For more details, see e.g. *Kevin Mitnick Case: 1999*. [online]. [cit.2.11.2011]. Available from: <http://www.encyclopedia.com/doc/1G2-3498200381.html>

[3] For more details see:

MITNICK, Kevin D. and William L., SIMON. *The Art of Deception (Uměniklamu)*. Gliwice: Helion, 2003. ISBN 83-7361-210-6.

MITNICK, Kevin D. *The art of intrusion: the real stories behind the exploits of hackers, intruders & deceivers*. Indianapolis: Wiley, 2006. ISBN 0-471-78266-1.

MITNICK, Kevin D. and William L., SIMON. *Ghost in the Wires: my adventures as the world's most wanted hacker*. New York: Little, Brown & Co, 2012. ISBN 9780316037723.

[4] *The testimony of an ex-hacker*. [online]. [cit.26.9.2008]. Available from:  
<http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/testimony.html>

[5] The example is literally cited from: MITNICK, Kevin D. and William L. SIMON. *The Art of Deception (Umění klamu)*. Gliwice: Helion, 2003. ISBN 83-7361-210-6, pp. 127–130

[6] **Enumeration** – a process that reveals the service enabled on the target system, the operating system platform, and a list of accounts names of the users who have access to the system.

[7] **Brute force attack** – a password detection strategy that consists of testing all possible combinations of alphanumeric and special characters.

## 4.2. Botnet

Botnet can be simply defined as a network of software-linked bots [1] that perform an action based on a command from the "owner" (or administrator) of that network. The network built in this way can be used for legal activities (e.g. distributed computing) or for illegal activities (see below).

It was the distributed calculations that, in fact, inadvertently gave criminals the idea of building botnets the way they are understood today. The following text is from a website about distributed computing: **"Most computers in the world use their full computing potential for only a very small part of their operating time, but their electricity consumption is only slightly lower than if they were fully utilised. It's a shame not to use this lounging computer, and very few people realise how much such unused power there is in the world... In distributed computing, the saying "There's no need for a shower, a few drops help too" applies in full, and drops from millions of ordinary computers in the world exceeds several times the performance of even the largest supercomputers in the world... Involvement in any distributed computing project consists only in the installation of the client, and it can usually perform all the necessary activities and take care of specific applications... Most projects work so that the total work is divided into lots of parts and these are then sent to individual computers, which request them. After processing each piece, the individual computers themselves send the resulting data back to the project centre, where the results are combined again into one unit."** [2]

The very idea of resource distribution, or the use of low computing power of other computer systems, for example for calculating complex mathematical algorithms, etc., is definitely not bad and is much more efficient than the use and construction of "supercomputers". However, as humans we are very inventive, so it was obvious that this idea would be used for purposes other than altruism or charity. The ability to distribute different tasks among different geographically located computers has been and is attractive to attackers.

The current computer system, for example, in the form of a mail server, has no problem sending tens of millions or billions of e-mail messages a day. If a user decides to use this system, for example, to spread spam, this computer system (traceable by identifiers such as IP address) will perform this activity only for a very short time as it will be blocked very soon by the ISP (e.g. due to illegitimate or excessive traffic in the network, which can be marked as spam); its address will appear on the "blacklists", and based on this information traffic will be blocked (e.g. outgoing mail). However, if an attacker uses distributed power in the form of a botnet, he will have thousands to hundreds of thousands of computers, each of which sends a portion of messages (e.g. 1000–2000 messages per day). Such traffic will then not be considered problematic and will not be stopped.

It is typical for a **botnet** that if **a target computer system is infected, this system**, called "zombie" or "bot", **connects to a central control server** [called a command-and-control server (C&C)]. **The whole system** (containing zombies and C&C) **is controlled by an attacker** (referred to as a botmaster or botherder) **who controls the bots via a C&C server.** [3]

The following elements are characteristic (necessary) for the botnet:

### 1. Command-and-control infrastructure (C&C)

It is infrastructure that consists of a control element (or elements) and bots (controlled by computer systems).

### 2. Installation and control of a bot

This is most often malware that is spread through a botnet or otherwise. The primary goal of such malware is to integrate other computer systems into a botnet. Malware exploits various vulnerabilities in computer systems.

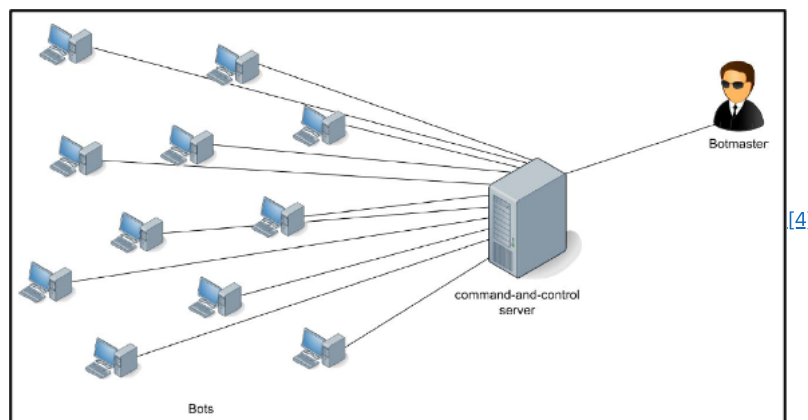
### 3. Controlling bots through C&C infrastructure

A bot is software that works secretly and uses common communication channels (IRC, IM, RFC 1459, etc.) to communicate with a C&C server. New bots try to get as much information as possible from their surroundings and promote themselves to other computer systems.

Based on the architecture, there are botnets with:

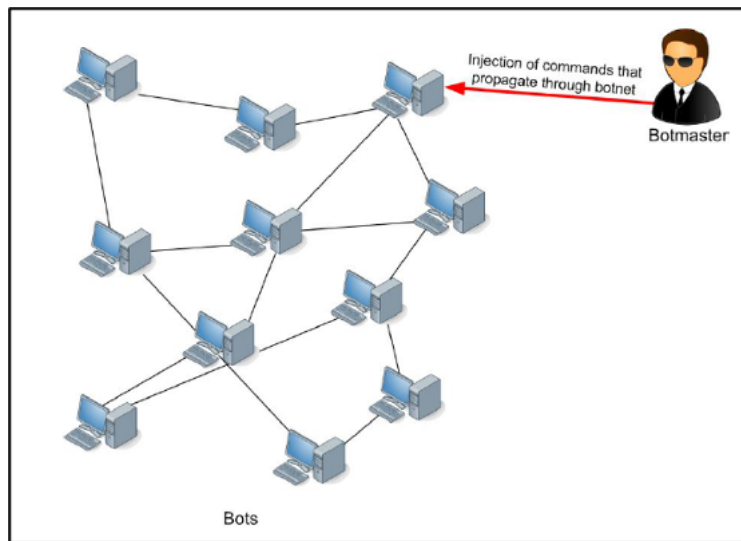
#### 1. Centralised architecture

This architecture is typically built on the principle of client-server communication. End computer systems (zombies/bots) communicate directly with the C&C server (central control element) and follow instructions and use resources from this server.



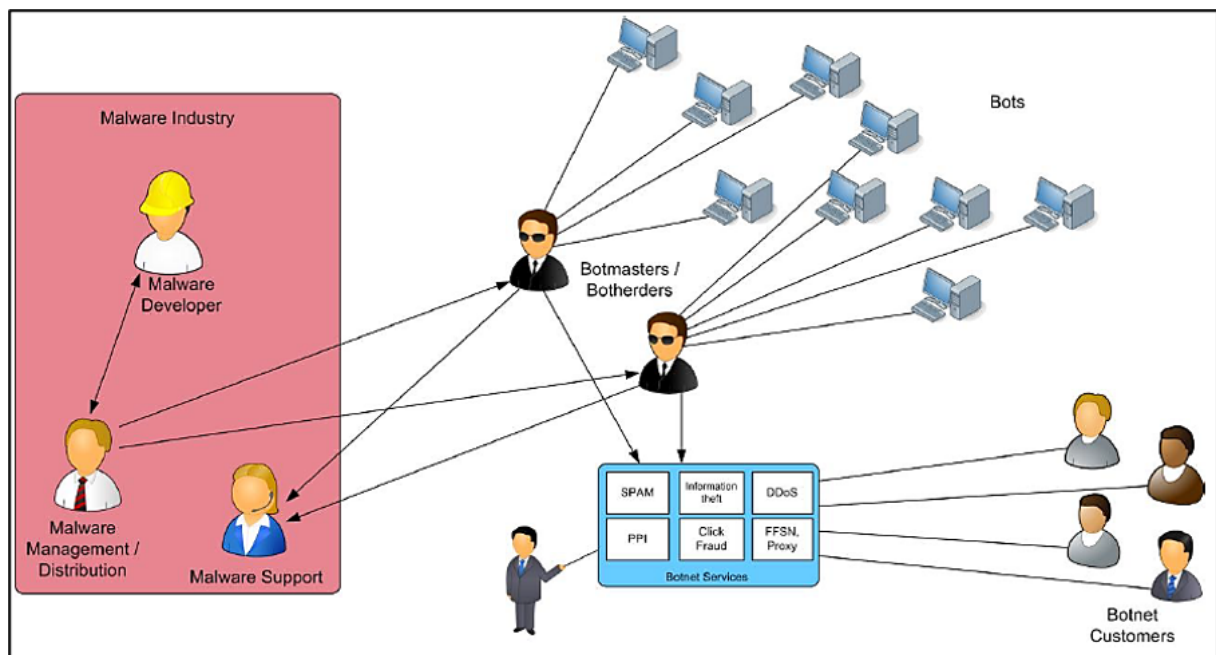
#### 2. Decentralised architecture

It is typically built on peer-to-peer (P2P) architecture. This architecture allows resources and commands to be shared within a P2P network. There is no central control element in the "classic" form, which makes this system more resistant to the attempt to take control through this control element.



[5]

Botnets can be used for many activities, but financial gain is mainly in the foreground, which consists in generating their own attacks (e.g. ransomware, phishing, spam, stealing information, DDoS, etc.), as well as renting their services or the entire botnet to clients. Thanks to the above, it is possible to include the botnet in the structure of **crime-as-a-service** (where the service is offered: **botnet-as-a-service**), or in the malware economy [6], where it represents the basic technical platform necessary to perform a number of cyberattacks.



Malware economy

The computer system that becomes part of the botnet is then typically used for one of the activities described in the following table. It should be noted that these attacks are usually combined or distributed within the botnet with respect to its occupancy, demand from "customers", etc.

Sending of	Identity Theft	DoS Attacks	Click Fraud
<ul style="list-style-type: none"> <li>- spam</li> <li>- phishing</li> <li>- malware</li> <li>- adware</li> <li>- spyware</li> </ul>	Personal and sensitive data and information is obtained and sent (back to the attacker). <ul style="list-style-type: none"> <li>- Account access data</li> <li>- Access data to e-mails, social networks, etc.</li> <li>- other data or information that may be used or sold by the attacker</li> </ul>	Launching a DoS attack against a target (computer system) specified by the botmaster.	The computer system displays (or clicks on) advertising links on the site without the user's knowledge. This gives the impression that the site has traffic and advertisers are losing money. [7]

In the table below I summarise a list of some known botnets [8]:

Creation date	End date	Name	Estimated number of bots	Number of spam in billions per day	Alias (also known as)	More information

<b>2002</b>						
	2011	<a href="#">Coreflood</a>	2,300,000			Backdoor. Collection of personal and sensitive information.
<b>2004</b>						
		<a href="#">Bagle</a>	230,000 <sup>[16]</sup>	5.7	Beagle, Mitglieder, Lodeight	Massive sending of spam. Designed for computer systems with Windows OS.
		Marina Botnet	6,215,000 <sup>[16]</sup>	92	DamonBriant, BOB.dc, Cotmonger, Hacktool.Spammer, Kraken	
		<a href="#">Torpig</a>	180,000 <sup>[17]</sup>		Sinowal, Anserin	Distribution of malware and collection of sensitive and personal data. Designed for computer systems with Windows OS.
		<a href="#">Storm</a>	160,000 <sup>[18]</sup>	3	Nuwar, Peacomm, Zhelatin	Sending of spam. Designed for computer systems with Windows OS.
<b>2006</b>						
	March 2011	<a href="#">Rustock</a>	150,000 <sup>[19]</sup>	30	RKRustok, Costrat	Sending of spam. Capable of sending up to 25,000 spam messages per hour from one computer. Active on Windows OS.
		<a href="#">Donbot</a>	125,000 <sup>[20]</sup>	0.8	Buzus, Bachsoy	Sending mainly pharmaceutical spam.
<b>2007</b>						
		<a href="#">Cutwail</a>	1,500,000 <sup>[21]</sup>	74	Pandex, Mutant (related to: Wigon, Pushdo)	Sending of spam. By default, it uses the Pushdo Trojan to infect a computer system. Active on Windows OS.
		<a href="#">Akbot</a>	1,300,000 <sup>[22]</sup>			Backdoor, allowing you to take control of an infected computer. After installation, it collected data, stopped processes, or launched DDoS attacks.
March 2007	November 2008	<a href="#">Srizbi</a>	450,000 <sup>[23]</sup>	60	Cbeplay, Exchanger	Primarily sending spam. The Srizbi trojan was used to infect computer systems.
		<a href="#">Lethic</a>	260,000 <sup>[16]</sup>	2	none	Sending mainly pharmaceutical spam.
September 2007		dBot	10,000+ (Europe)		dentaoBot, d-net, SDBOT	
		<a href="#">Xarvester</a>	10,000 <sup>[16]</sup>	0.15	Rlsloup, Pixeliz	Sending of spam.
<b>2008</b>						

		<a href="#">Sality</a>	1,000,000 <sup>[24]</sup>		Sector, Kuku	Malware group. Computer systems infected with Sality communicate through P2P. The activity consists of: sending spam, collecting sensitive data, attacking web servers, performing distributed calculations (e.g. for password cracking, etc.).  Active on Windows OS.
April 2008		<a href="#">Kraken</a>	495,000 <sup>[33]</sup>	9	Kracken	Malware distribution. Connecting other computers to the botnet.
	December 2009	<a href="#">Mariposa</a>	12,000,000 <sup>[25]</sup>			Botnet primarily involved in scam and DDoS attacks. <b>It was one of the biggest botnets ever.</b>
November 2008		<a href="#">Conficker</a>	10.500,000+ <sup>[26]</sup>	10	DownUp, DownAndUp, DownAdUp, Kido	Worm attacking computer systems with Windows OS.  The bugs of this OS were used to further expand the botnet.
November 2008	March 2010	<a href="#">Waledac</a>	80,000 <sup>[27]</sup>	1.5	Waled, Waledpak	Sending of spam and distribution of malware. Terminated by Microsoft action.
		Maazben	50,000 <sup>[16]</sup>	0.5	None	Sending of spam, malware, scam, phishing.
		OnewordSub	40,000 <sup>[28]</sup>	1.8		
		Gheg	30,000 <sup>[16]</sup>	0.24	Tofsee, Mondera	
		Nucrypt	20,000 <sup>[28]</sup>	5	Loosky, Locksky	
		Wopla	20,000 <sup>[28]</sup>	0.6	Pokier, Slogger, Cryptic	
		<a href="#">Asprox</a>	15,000 <sup>[29]</sup>		Danmec, Hydraflux	Phishing attacks, SQL injections, spread of malware.
		<a href="#">Spamthru</a>	12,000 <sup>[28]</sup>	0.35	Spam-DComServ, Covesmer, Xmiler	Using P2P
	19/07/2012	<a href="#">Grum</a>	560,000 <sup>[31]</sup>	39.9	Tedroo	Sending mainly pharmaceutical spam.
		<a href="#">Gumblar</a>				
<b>2009</b>						
May 2009	November 2010	<a href="#">BredoLab</a>	30,000,000 <sup>[30]</sup>	3.6	Oficla	Sending of spam. Ended by a joint action of the Dutch police, Govcert NL, Europol. Kaspersky Lab etc. <b>Probably the largest known botnet.</b>

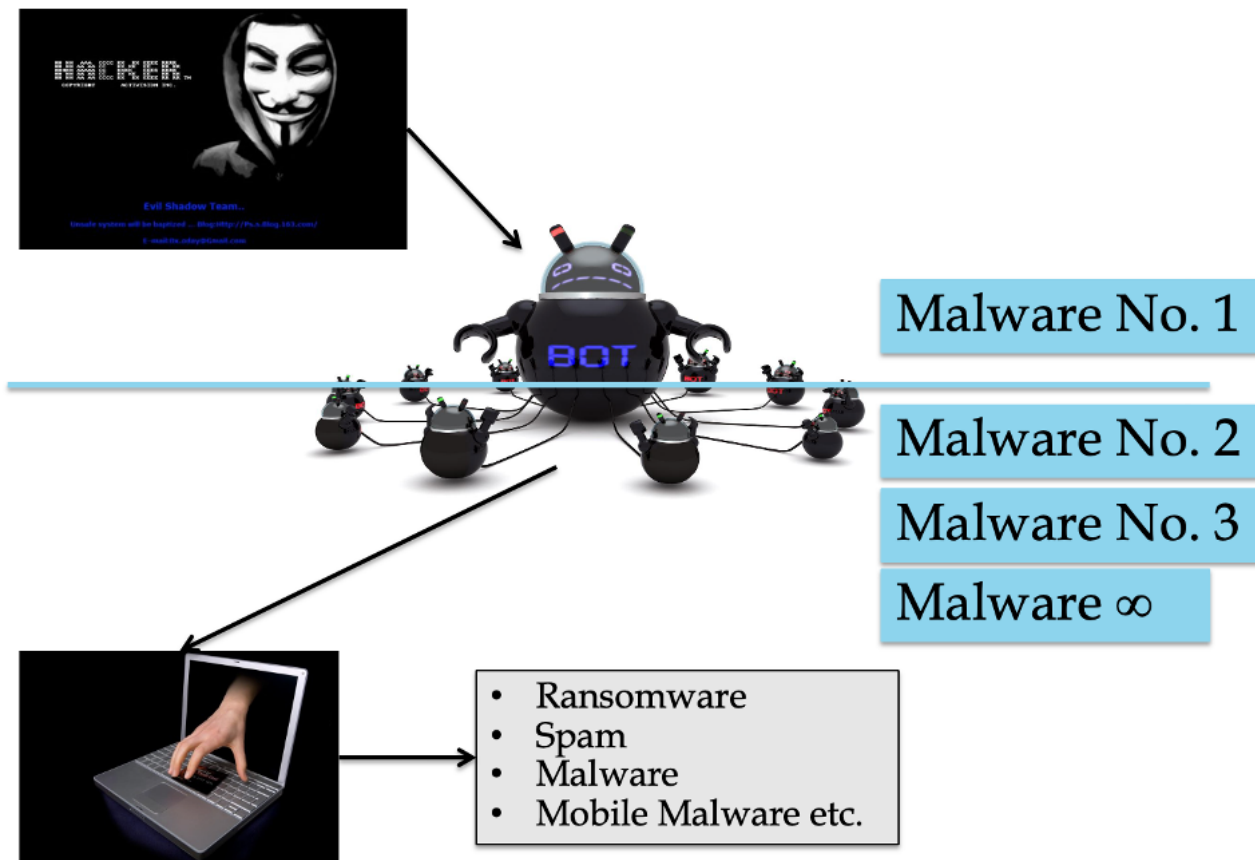
	November 2009	<a href="#">Mega-D</a>	509,000 <sup>[32]</sup>	10	Ozdok	Sending of spam.
	August 2009	<a href="#">Festi</a>	250,000 <sup>[34]</sup>	2.25	Spamnost	Sending spam and performing DDoS attacks.
<b>2010</b>						
	January 2010	LowSec	11,000+ <sup>[16]</sup>	0.5	LowSecurity, FreeMoney, Ring0.Tools	
		<a href="#">TDL4</a>	4,500,000 <sup>[35]</sup>		TDSS, Alureon	
		<a href="#">Zeus</a>	3,600,000 (US only) <sup>[36]</sup>		Zbot, PRG, Wsnpoem, Gorhax, Kneber	Focused on activities related to the theft of bank account information. It also installed CryptoLocker ransomware, etc. Active on Windows OS.
	(Several: 2011, 2012)	<a href="#">Kelihos</a>	300,000+	4	Hlux	Mostly involved in Bitcoin theft and sending spam.
<b>2011</b>						
	2015-02	<a href="#">Ramnit</a>	3,000,000 <sup>[37]</sup>			Worm attacking computer systems with Windows OS. Terminated by a joint action of Europol and Symantec.
		<a href="#">Zero Access</a>	2,000,000		Max++ Sirefef	Botnet used mainly for mining bitcoins and click fraud.  Active on Windows OS.
<b>2012</b>						
		<a href="#">Chameleon</a>	120,000		None	Click Fraud
		<a href="#">Nitol</a>				Botnet involved in the spread of malware and DDoS attacks. Most zombies (up to 85%) are located in China. The botnet client was found in computer systems delivered directly from the factory.
<b>2013</b>						
		Boatnet	500+ server computers	0.01	YOLOBotnet	
		Zer0n3t	200+ server computers	4	FiberOptck, OptckFiber, Fib3rl0g1c	
<b>2014</b>						
		<a href="#">Semalt</a>	300,000+		Soundfrost	Sending of spam.
		<a href="#">Necurs</a>	6,000,000			
<b>2016</b>						
		<a href="#">Mirai</a>	380,000			DDoS, sending of spam.

		<b>Methbot</b>	6,000 domains and 250,267 distinct URLs			
<b>2018</b>						
		<b>3ve</b>	1.7 million computers and a large number of servers			Money theft.

In fact, any computer system can be connected to a botnet network. Among other things, these are systems that satisfy the requirements of IoT (Internet of Things). In 2014, a case was reported in which a botnet included a fridge sending out more than 750,000 spam e-mails. [9].

The Nigam study shows [10] that there are dozens of botnets directly created and primarily focused on computer systems, which we can call mobile devices (e.g. smartphones, tablets, etc.). Due to the installation of applications from unknown sources and the considerable absence of antivirus products on users' mobile devices, it is also much easier to install malware on these mobile devices and thus gain control over them. These devices are currently able to fully meet the requirements of a botmaster for the operation of a botnet, or for the tasks assigned to "zombies".

Malware serves as a means of gaining access, control, and further spread of malware or other tasks as directed by an attacker, and not only in the case of botnets. However, if malware is currently infected on a user's computer system, it is highly likely that it has become part of the botnet. An attacker (botmaster) installs malware on a computer system (zombie) that allows him to manipulate the computer system remotely (malware No. 1 – while this malware leaves control to the botmaster even if, for example, part or all of the botnet is leased). Only then is another malicious software (malware 2. to malware ∞) installed to perform other tasks (e.g. sending spam, collecting data, extortion using ransomware, etc.). The whole structure can be illustrated as follows:



Malware installed on a computer system connected to a botnet

From a legal perspective, it can be stated that botnets represent entire networks of infected computer systems over which a third party has taken over some control without authorisation, without the knowledge of authorised users. Such infected systems most often serve as a base for anonymous connection of an attacker to the Internet, for sending malicious programs, carrying out attacks on other targets, carrying out DoS attacks, spreading spam, identity theft or other cyberattacks.

### Possibilities of criminal sanctions in the Czech Republic

As for an attacker's own activity, which consists in the installation of malware for the subsequent control of a computer system, it is possible to assess this conduct according to **Section 230** of the Criminal Code (Unauthorised access to the computer system and information carrier). If an attacker put malware into a computer system with the intention of causing damage or other harm to another or gaining an unauthorised benefit to himself or another,



his actions could be qualified according to Section 230 (2) (d) of the Criminal Code.

It can be argued that it is also an unauthorised use of another's possession (because the computer system in question is another's possession in these cases) under **Section 207 (1) al. (1)** of the Criminal Code. Application of Section 207 (1) al. (2) of the Criminal Code [11], can be quite problematic, as the intensity of intervention and use of the computer system is decisive. On the basis of this degree of intensity, it would be possible, if appropriate, to quantify the damage incurred as an expression of depreciation at the time of use. Unfortunately, when using this calculation the caused damage is not small.

The actual protection against connection and use of computers within the botnet can have two levels. The first level is to increase the protection of property rights by supplementing Section 207 of the Criminal Code with the basic objective element, the wording of which could be as follows: **"Who will use a computer system without the consent of the entitled person."**

This provision would also define the circumstance which consists in interfering with the ownership rights of another. In the case of unauthorised use of another's possession in relation to a computer system, the solution is not to reduce the damage from not small to insignificant (see Section 207 (1) al. (1) of the Criminal Code, as the price of many computer systems is currently lower than at least CZK 5,000), and yet these computer systems are able to fully perform the assigned activity within the botnet.

The second level, which describes the seriousness of the attacker's actions, then consists in the inclusion of a new qualification circumstance in Section 230 (3) of the Criminal Code, while this circumstance could be as follows:

**"intentionally connects a computer system to a computer network with the intention of committing a crime or uses it on that network with the same intention"**

### Possibilities of criminal sanctions in Poland

Illegal access to a system (hacking) - Art. 267 § 1 and 2 of the Penal Code. This crime is prosecuted at the request of the aggrieved party. They are punishable by a fine, restriction of liberty or imprisonment for up to 2 years.

Article 267 Unlawful obtaining of information

§ 1. Whoever, without authorisation, gains access to information not intended for him, by opening a closed magazine, connecting to a telecommunications network or breaking or bypassing electronic, magnetic, IT or other specific protection thereof, shall be subject to a fine, the penalty of limitation of liberty or deprivation of liberty for up to 2 years.

§ 2. The same punishment shall be imposed on anyone, who without authorisation, gains access to the whole or any part of an IT system.

§ 3. The same punishment shall be imposed on anyone, who in order to obtain information to which he is not entitled, establishes or uses an eavesdropping or visual device, or other device or software.

§ 4. The same punishment shall be imposed on anyone who discloses information obtained in the manner specified in § 1-3 to another person.

§ 5. The prosecution of the offence specified in § 1-4 shall occur on the motion of the injured person.

### Possibilities of criminal sanctions in Portugal

According to Art. 6(2) of the *Cybercrime Law*, the illegal introduction in one or several computer devices of any computer programme, executable instruction, code or data intended to perform an illegal to a computer system is penalised as being an Illegal access. The same goes for the crimes of Damage to computer programmes or other computer data [Data interference] (Art. 4(3), Computer sabotage [Illegal interference] (Art. 5(2) and also Illegal interception (Art. 7(3)).

Besides, there are not in place any provisions related to the building or use of networks for performing any of the stated offence.

---

[1] **Bot** (abbreviation of the word robot). It is a program that can execute an attacker's commands entered from another computer system. Most often it is an infection of a computer with a virus such as worm, Trojan horse, etc. The computer system, which is thus remotely controlled, is then referred to as a **zombie**. However, some sources even refer to an infected computer system as a bot.

A bot can collect data, process requests, send messages, communicate with a control element, etc.

[2] For more details see *Distribuvanévypočty*. [online]. [cit.2.11.2013]. Available from: <http://dc.czechnationalteam.cz/>

[3] For more details see: PLOHMANN, Daniel, Elmar GERHARDS-PADILLA and Felix LEDER. *Botnets: Detection, Measurement, Disinfection & Defence*. ENISA, 2011. [online]. [cit.17.5.2015], p. 14. Available from: <https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence>

Further botnet definitions and information about them can be found, for example, at:

*Co je to botnet a jak se šíří?*[online]. [cit.15.7.2016]. Available from: <https://www.youtube.com/watch?v=ywXqDon5Xtg>

*Botnety: nová internetová hrozba*. [online]. [cit.15.7.2016]. Available from: <http://www.lupa.cz/clanky/botnety-internetova-hrozba/>

*Války síťových robotů – jak fungují sítě botnets*. [online]. [cit.15.7.2016]. Available from: [http://tmp.testnet-8.net/docs/h9\\_botnet.pdf](http://tmp.testnet-8.net/docs/h9_botnet.pdf)

*Botnets*. [online]. [cit.15.7.2016]. Available from: <https://www.youtube.com/watch?v=-8FUstzPixU&index=2&list=PLz4vMsOKdWVHb06dLjXS9B9Z-yFbzUWI6>

[4] Figure of a centralised botnet. For more details see: PLOHMANN, Daniel, Elmar GERHARDS-PADILLA and Felix LEDER. *Botnets: Detection, Measurement, Disinfection & Defence*. ENISA, 2011. [online]. [cit.17.5.2015], p. 16. Available from: <https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence>

[5] Figure of a decentralised botnet. Ibidem, p. 18

[6] Malware economy. For more details see: PLOHMANN, Daniel, Elmar GERHARDS-PADILLA and Felix LEDER. *Botnets: Detection, Measurement, Disinfection & Defence*. ENISA, 2011. [online]. [cit.17.5.2015], p. 21. Available from: <https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence>

[7] *Bots and Botnets – A growing Threat*. [online]. [cit.11.8.2016]. Available from: <https://us.norton.com/botnet/>

[8] The table was created based on a combination of information from the following sources:

*Botnet*. [online]. [cit.15.7.2016]. Available from: <https://en.wikipedia.org/wiki/Botnet>

*Botnet – Historical List of Botnets*. [online]. [cit.15.8.2016]. Available from: [http://www.liquisearch.com/botnet/historical\\_list\\_of\\_botnets](http://www.liquisearch.com/botnet/historical_list_of_botnets)

*Botnet*. [cit.8.7.2016]. Available from: <http://research.omicsgroup.org/index.php/Botnet>

*Historical list of botnets*. [online]. [cit.15.8.2016]. Available from: <http://jpdias.me/botnet-lab/history/historical-list-of-botnets.html>

[9] *Fridge caught sending spam e-mails in botnet attack*. [online]. [cit.17.5.2016]. Available from: <http://www.cnet.com/news/fridge-caught-sending-spam-emails-in-botnet-attack/>

[10] For more details see NIGAM, Ruchna. *A timeline of Mobile Botnets*. [online]. [cit.12.7.2016]. Available from: <https://www.botconf.eu/wp-content/uploads/2014/12/2014-2.2-A-Timeline-of-Mobile-Botnets-PAPER.pdf>

[11] This provision provides for damage to other people's property, while the damage does not have to be small (i.e. at least CZK 25,000, see Section 138 (1) of the Criminal Code).

## 4.3. Malware

**Malware** (a compound of malicious software) can be any software used to disrupt the standard operation of a computer system, gain information (data) or used to gain access to a computer system. Malware can take many forms, with many types of malware named after the activity they perform.

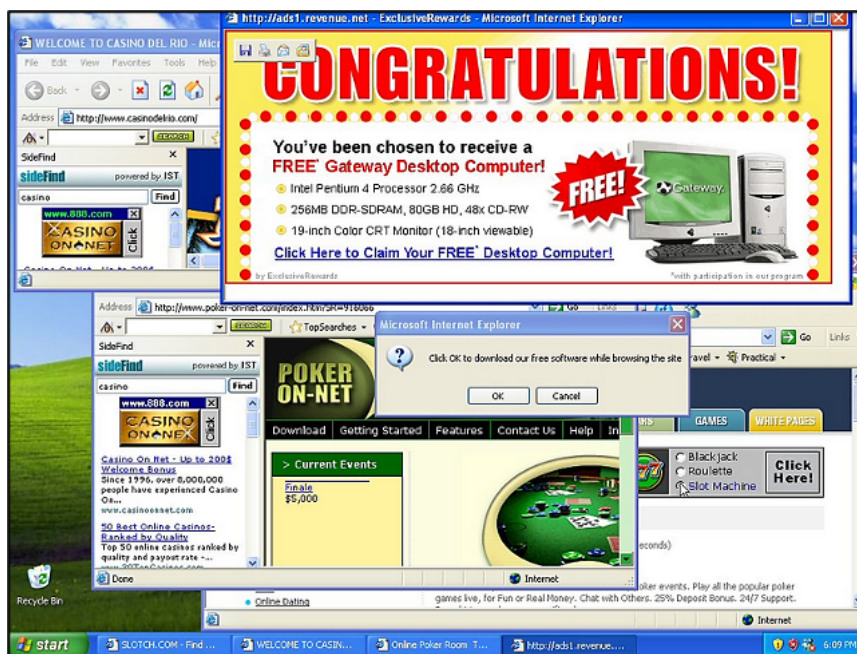
One malware is able to perform several functions (carry out several activities) at once. For example, it can further spread itself via e-mails (in an attachment) or as data in P2P networks, and at the same time it can obtain, for example, e-mail addresses from an infected computer system.

Historically, there were at first a number of different terms for this software, which is currently referred to by the collective term malware. The actual names of specific malicious software were usually created according to the activity that the program performed. Despite the above statement that the term malware is primarily used at present, it is still possible to come across a historically older designation of malicious software. These are the following groups:

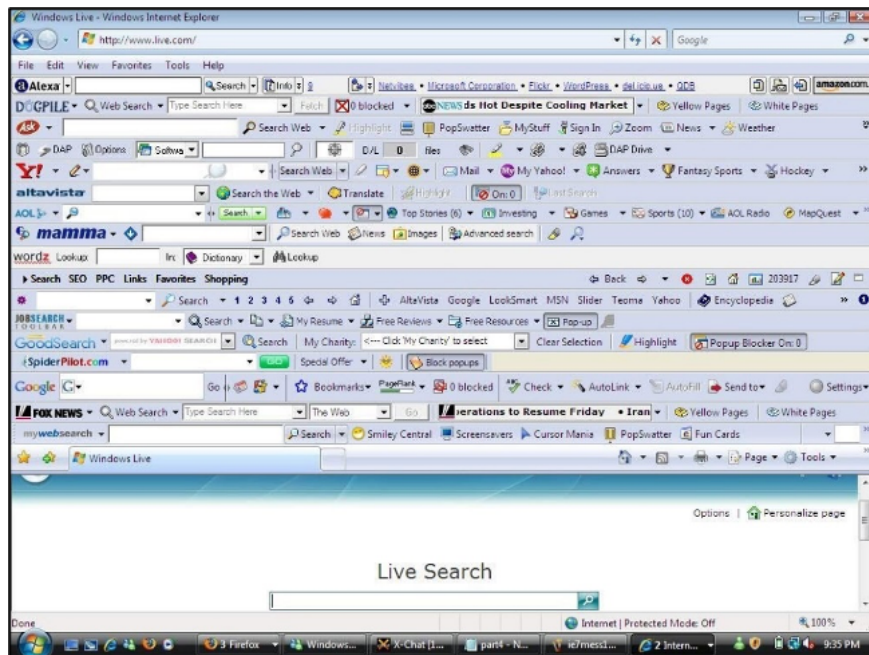
1. **Adware**
2. **Spyware**
3. **Viruses**
4. **Worms**
5. **Trojan Horses**
6. **Backdoor**
7. **Rootkits**
8. **Keylogger**
9. **Ransomware etc.**[1].

### Ad 1) Adware

The term adware is an abbreviation of the English phrase *"advertising supported software"*. It is the least dangerous but profitable form of malware.[2]. Adware displays advertisements on the user's computer system (e.g. pop-ups in the operating system,[3] or on websites, advertisements displayed together with software, etc.). Although in most cases these are products that only bother the user with constant advertising messages that "pop up" on the screen, adware can also be associated with spyware, the purpose of which is to monitor user activity and steal important information.



Adware



Example of Adware and other add ons installed in a web browser [4]

## Ad 2) Spyware

The term spyware is a combination of the English words "spy" and "software". Spyware is used to obtain statistical data [5] on an operation of a computer system and to send it to an attacker's data box without a user's knowledge and consent. This data may also include information of a personal nature or information about a person of a user, as well as information about visited websites, running applications, etc.

Spyware can be installed as a standalone malware, as well as often as part of other, free and otherwise completely safe programs. In this case, the installation and other activities of the spyware are typically handled in the terms of the EULA, and the user usually unknowingly voluntarily agrees to monitor their own activities. Adding spyware programs to other programs (e.g. P2P client programs, various shareware programs, etc.) is motivated by the program manufacturer's efforts to find out the interests or needs of a user and use this information, for example, for targeted advertising. [6] A characteristic feature of spyware programs that are part of a "program package" is that they usually remain installed on the computer even after the main program has been uninstalled, which in most cases is hidden from the user.

Spyware poses a threat both because it sends various information from a user's computer system to an "attacker" (which is further processed and correlates with data and information obtained from other sources), and because spyware may contain other tools that affect the user's own activities. [7]

## Ad 3) Viruses

It is a program or malicious code that attaches itself to another existing executable file (e.g. software, etc.) or document. The virus is reproduced the moment this software is launched or an infected document is opened. Most often, viruses spread through the sharing of software between computer systems; they do not need the cooperation of a user to spread them. Viruses were the dominant form of malware, especially in the 1980s and 1990s. [8]

There are a large number of viruses whose purpose is to destroy, while others are designed to "settle" in as many computer systems as possible and then use them for a targeted attack. Typical for these programs is the ability to spread between systems without the need for user intervention on a computer system. Effects of viruses can be multifarious, such as the harmless playing of a melody, system congestion, change or destruction of data, or the total destruction of an infected system. Computer viruses can be classified according to many different aspects, e.g. according to the host (i.e. according to the type of programs that computer viruses transmit), according to the ways they effect in the system, according to their location in memory, etc. [9] Depending on what files the viruses infect, they can be divided into:

- boot viruses (infect only system partitions)
- file viruses (infect only files)
- multipartite viruses (infect files as well as system areas)
- macroviruses (attack applications using macros)

## Ad 4) Worms

So-called **computer worms** are also referred to as viruses. The reason for the closer connection with viruses is the fact that worms do not need any host, i.e. no executable file (similar to viruses). Unlike viruses, which are attached as part of another program, these programs usually spread separately. A compromised system is then used by a worm to further send copies of itself to other users via network communication. In this way, it spreads very quickly, which can lead to congestion of a computer network, and thus an entire infrastructure. Unlike viruses, these programs are able to analyse security vulnerabilities in the security of an infected information system, [10] so they are also used to look for security gaps in systems or mail programs. [11]

## Ad 5, 6) Trojan Horses and Backdoors

**Trojan horses** are generally those computer programs that contain hidden features that a user does not agree with or is unaware of, and that are potentially dangerous to the continued operation of a system. As with viruses, these programs can be attached to another, secure program or application, or they can look like a harmless computer program. Trojan horses, unlike classical viruses, are unable to replicate or spread without

the "help" from a user. If a Trojan horse is activated, it can be used, for example, to delete, block, modify, copy data or disrupt the running of a computer system or computer networks.

Some Trojans, when activated without a user's knowledge, open the communication ports of a computer, which significantly simplifies further infection of the affected system by other malicious programs, or facilitates direct control of the infected computer so-called remotely. Such Trojan horses are referred to as **backdoor**.[\[12\]](#) Modern backdoor programs have improved communication and use most protocols of some communication tools, such as ICQ.[\[13\]](#)

The use of Trojan horses is often associated with the use of various **scanning** [\[14\]](#) **programs** ("port scanners"), which are programs that are used mainly to determine which communication network ports of the computer are open, what services are running on them and whether it is possible to carry out an attack on such a system. This data is again sent to an attacker and is also potentially useful in committing other cyberattacks.

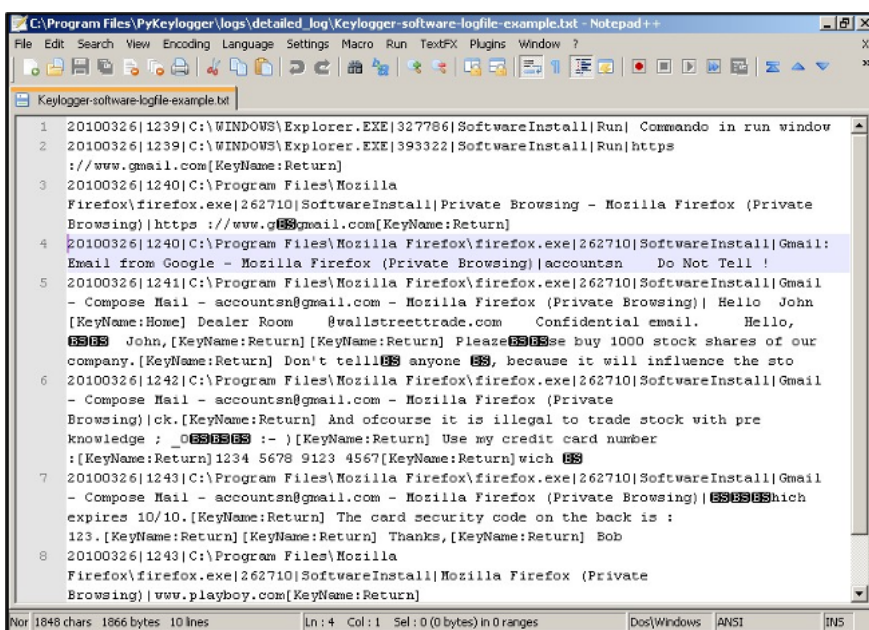
#### Ad 7) Rootkits

This term refers not only to computer programs, but also to the entire technology used to mask the presence of malware (e.g. computer viruses or Trojan horses, worms, etc.) in an infected system. They most often take the form of not very large computer programs. Rootkits are not harmful in themselves, but are used by the creators of malicious programs, such as viruses, spyware, etc..[\[15\]](#) A rootkit program changes the behaviour of an entire operating system, its parts, or add-on applications so that users do not become aware of the existence of malicious programs on their computer system. In general, rootkits can be divided into **system** (modifying the kernel) and **application** (modifying the application configuration) rootkits.[\[16\]](#)

Of the applications, rootkits mainly attack specialised programs for searching for and removing dangerous programs from the system, i.e. antivirus, etc.[\[17\]](#) When using a rootkit program, antivirus programs cannot remove this malicious program from the infected system. In this way, the presence of a malicious program in the infected system is prolonged. From this point of view, it can be stated that rootkits can be very easily misused to commit crimes related to the use or misuse of information technology. Some literature refers to these tools as a subgroup of backdoor Trojans.[\[18\]](#)

#### Ad 8) Keylogger (Keystroke Logger)

Keylogger is software that records specific keystrokes on an infected computer system. Most often, a keylogger is used to record login data (username and password) to accounts that are accessed from a computer system. The information obtained is then typically sent to an attacker.



```
C:\Program Files\PyKeylogger\logs\detailed_log\Keylogger-software-logfile-example.txt - Notepad++
File Edit Search View Encoding Language Settings Macro Run TextFX Plugins Window ?
Keylogger-software-logfile-example.txt
1 20100326|1239|C:\WINDOWS\Explorer.EXE|327786|SoftwareInstall|Run| Commando in run window
2 20100326|1239|C:\WINDOWS\Explorer.EXE|393322|SoftwareInstall|Run|https
  ://www.gmail.com[KeyName:Return]
3 20100326|1240|C:\Program Files\Mozilla
  Firefox\firefox.exe|262710|SoftwareInstall|Private Browsing - Mozilla Firefox (Private
  Browsing)|https ://www.g[REDACTED]gmail.com[KeyName:Return]
4 20100326|1240|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail:
  Email from Google - Mozilla Firefox (Private Browsing)|accounts[REDACTED] Do Not Tell !
5 20100326|1241|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail
  - Compose Mail - accounts[REDACTED]gmail.com - Mozilla Firefox (Private Browsing)| Hello John
  [KeyName:Home] Dealer Room @vballstreettrade.com Confidential email. Hello,
  [REDACTED] John,[KeyName:Return][KeyName:Return] Please[REDACTED]buy 1000 stock shares of our
  company.[KeyName:Return] Don't tell[REDACTED]anyone [REDACTED], because it will influence the sto
6 20100326|1242|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail
  - Compose Mail - accounts[REDACTED]gmail.com - Mozilla Firefox (Private
  Browsing)|ck.[KeyName:Return] And ofcourse it is illegal to trade stock with pre
  knowledge ; _[REDACTED] :- ) [KeyName:Return] Use my credit card number
  : [KeyName:Return]1234 5678 9123 4567 [KeyName:Return]wich [REDACTED]
7 20100326|1243|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail
  - Compose Mail - accounts[REDACTED]gmail.com - Mozilla Firefox (Private Browsing)|[REDACTED]which
  expires 10/10.[KeyName:Return] The card security code on the back is :
  123.[KeyName:Return][KeyName:Return] Thanks,[KeyName:Return] Bob
8 20100326|1243|C:\Program Files\Mozilla
  Firefox\firefox.exe|262710|SoftwareInstall|Mozilla Firefox (Private
  Browsing)|www.playboy.com[KeyName:Return]
```

Example of keylogger operation.[\[19\]](#)

#### Ad 9) Ransomware

Ransomware will be described in more detail in a separate chapter.

#### Malware distribution

There are a number of ways in which malware can be delivered to a target computer system. Here I will briefly list some methods of spreading malware. Malware can be distributed through:

- **Portable storage media**

For example, using CD, DVD, USB, external drive, etc. This is the oldest but still effective way of distributing malware, where users pass infected files or **computer networks** containing **infected files** (sharing such files within computer networks, typically P2P networks).

- **Drive-by-download**

One of the most common ways to infect malware is to download it from the Internet and then run a file, typically with an .exe (executable file) extension, from an unknown source. These can be fake or counterfeit programs (e.g. imitations of Flapp Bird, fake media codecs, etc.), programs used to circumvent copyright protection (cracks, keygens, etc.), real infected programs, etc.

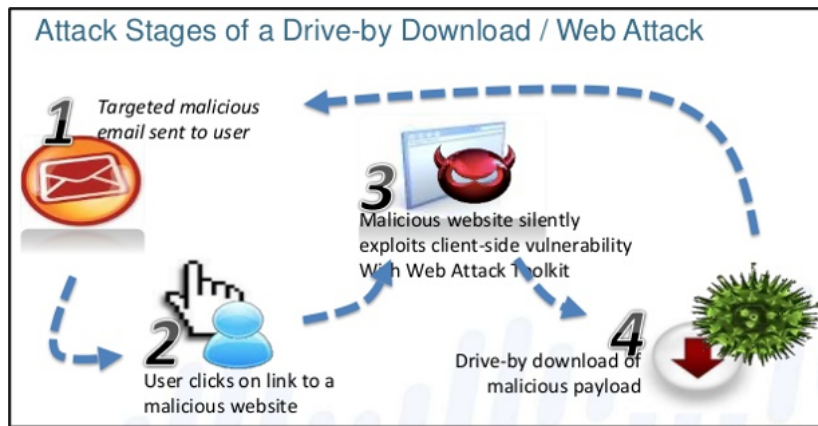
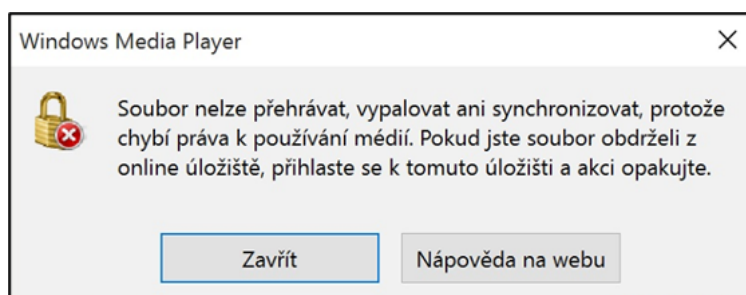
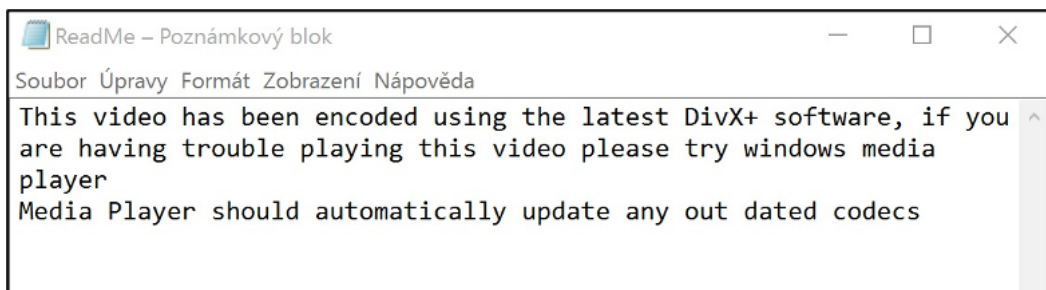
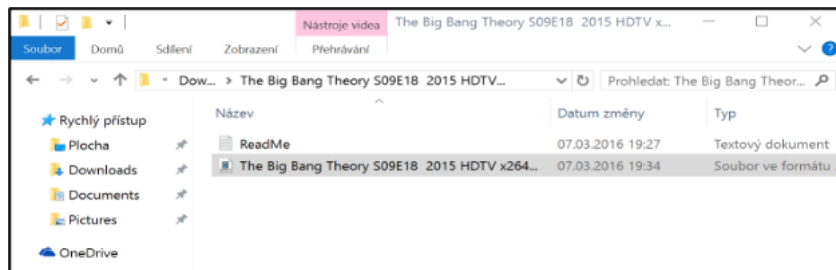


Illustration of one of the possible principles of drive by download. [20]

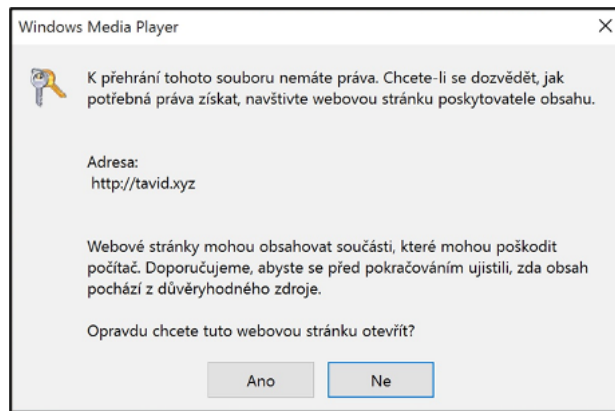
The following example shows malware downloaded by a user through a P2P network (specifically, a file featuring *The Big Bang Theory –Season 9, Part 18*). This malware prompted users to download a new codec through Media Player so that the video could be played. The media player started to connect to an attacker's site and then a fictitious codec was installed, but in fact malware was installed on the computer (in this case a combination of malware: backdoor, keylogger, bot), which allowed the attacker to completely control the user's computer system.

In this case, the fact that the offered part of *The Big Bang Theory* has not yet been broadcast in the USA, where it premieres, was very striking, but the number of downloads was in the tens of thousands.



Text on the figure: The file cannot be played, burned or synchronised because media usage rights are missing. If you received the file from an online repository, log in to that repository and try again.

Close / Help on the web



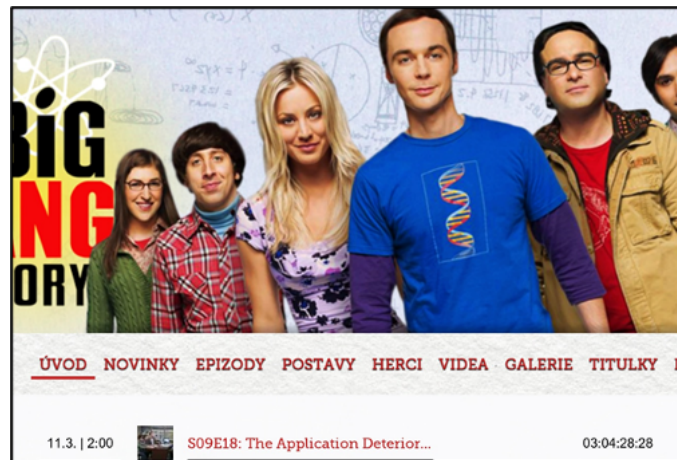
*Text on the figure: You do not have permission to play this file. To learn how to obtain the necessary rights, visit the content provider's website.*

Address: <http://tavid.xyz>

*Websites can contain components that can harm your computer. We recommend that you make sure that the content comes from a trusted source before proceeding.*

*Are you sure you want to open this web page?*

Yes / No



- **"Office documents"**

Very often, malware spreads in the body of files such as: .doc, .xls, .avi, etc. Only macro viruses can be distributed in this way. A user assumes that he/she is opening a word document, but at the same time runs an executable file that masquerades as that document.

- **E-mail**

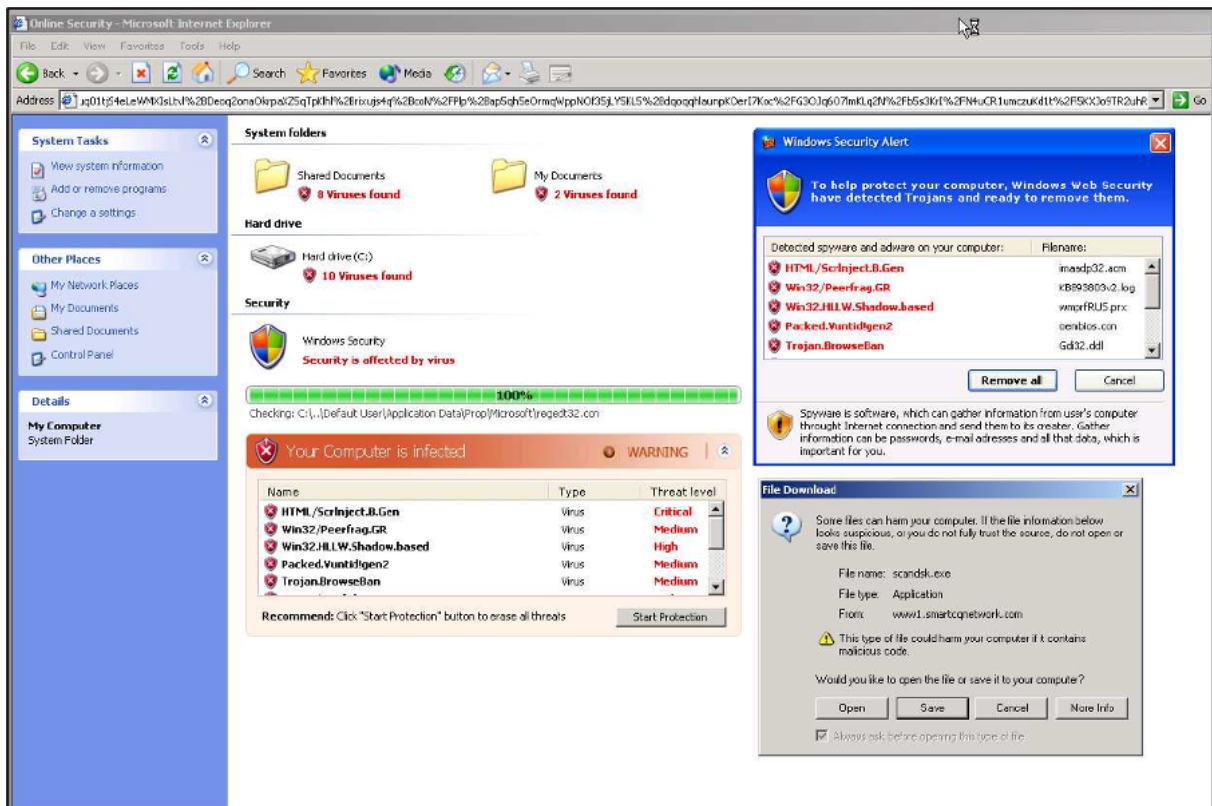
Malware can be stored in an attachment to an e-mail, or it can be a script inside a HTML\_[\[21\]](#) body of e-mails. This is currently one of the most common ways of distributing malware. Examples are current phishing campaigns, hoaxes, spam, etc.

- **HTML**

Malware can be placed directly on a website or in individual scripts.

- **Fake antivirus**

Users are typically offered a free antivirus – as adware. This antivirus will "scan your computer" and detect serious vulnerabilities and malware that a user's antivirus did not detect. Fake antivirus combines a social engineering attack (raising concerns about malicious software) with the installation of malware contained in a fake antivirus.



Fake antivirus




Fake antivirus. [22]

If a user is unsure whether a file or website contains malware, they can use a variety of tools to help them check for malware.

One of the proven services is <https://www.virustotal.com/>. On this webpage, a user can specify a scan of a file up to 128 MB or have a website he/she intends to access checked. (It is advisable to perform this scan, for example, when visiting Internet banking sites or payment sites. You need to copy the **full URL of the page you visit**.) The Virustotal service connects companies handling cybersecurity, the development of antivirus products, etc., while a user's request is tested by the tools of all these companies, thus increasing the probability of detecting malicious software.

The following printscreen shows the scan result of a newly delivered file as part of a phishing campaign. The day after the start of this campaign, only 5 companies identified malware in an attached file, and within a week all other companies were able to identify it. However, the time between the delivery of updates to users' antiviruses on their computer systems and the start of the attack is crucial for the eventual success of an attacker.





SHA256: 121a87042e9f8a5185e8e987eadc05d4b859498776f0f60d188f8e8bf3c89187

File name: ebill4290013.zip

Detection ratio: 5 / 56


Analysis date: 2015-01-12 08:10:15 UTC ( 1 rok, 7 měsíců ago )

0/0

Analysis Additional information Comments 0 Votes

Antivirus	Result	Update
CMC	Packed.Win32.Katusha.1!O	20150109
K7AntiVirus	Trojan ( 7000000c1 )	20150112
Norman	Kryptik.CEDX	20150112
Sophos	Troj/Invo-Zip	20150112
Symantec	Suspicious.Cloud.5	20150112
ALYac	✓	20150112
AVG	✓	20150112
AVware	✓	20150112

### File test result



URL: https://www.cubbyusercontent.com/pl/\_054c42bf3db94f20896a6c9445f647e4

Detection ratio: 3 / 66

Analysis date: 2016-02-02 19:24:03 UTC ( 0 minut ago )

Analysis Additional information Comments Votes

URL Scanner	Result
Sophos	Malicious site
ESET	Malware site
Emsisoft	Malware site
ADMINUSLabs	Clean site

### Website test result

**Malware can be installed on almost any computer system.** Micromalware installation cases are examples of specific installations. This is malicious code that spreads on a relatively small number of computer systems. This code exhibits abnormal behaviour and security programs often fail to respond. The most well-known case of micromalware is the **STUXNET** worm [23] or the installation of a botnet client in the already mentioned fridge.

A malware designed for mobile devices (**mobile malware**) is then a separate chapter. The first malware designed to attack mobile phones was discovered around 2004. Today, Kaspersky Lab, which reported on the discovery at the time, states that there are more than **340,000malware**. [24]

If we focus on the most vulnerable operating system within mobile devices, then most threats target the Android OS. The reason for this is mainly the variety of used operating system versions and their outdatedness. **Most Android devices do not allow you to update your operating system to the latest version, which is usually modified to withstand known vulnerabilities and has already fixed bugs from previous versions of this operating system. In fact, it is estimated that 77% of the threats attacking the Android OS could be eliminated by using the latest version of this operating system.**

In the case of mobile devices, attackers mainly use:

- **Outdated version of a mobile device operating system** (known vulnerabilities of individual systems);
- **Minimal security of a mobile device** by anti-virus means;
- **User ignorance** (Many users recklessly install applications "from an unknown source" or applications that require excessive access and permissions within the device.);
- **Social engineering and "waves of interest" in applications of a certain type.**

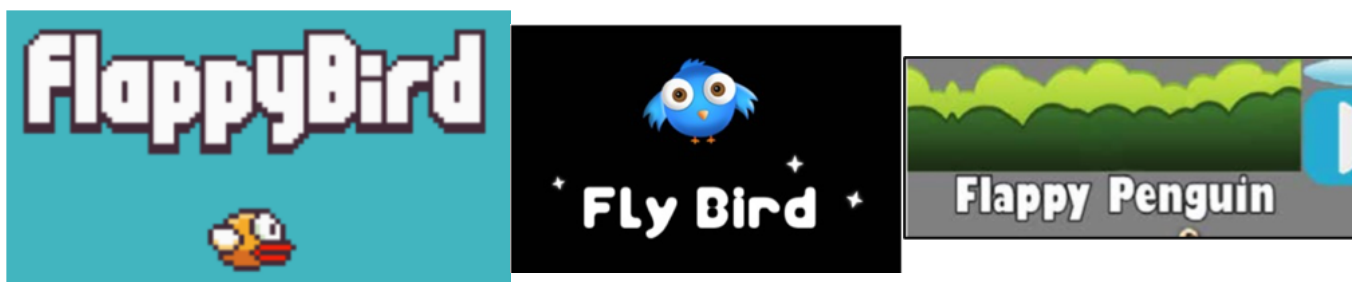
One of the reasons why Android is attacked as the primary operating system is the fact that the security of applications is not verified within the distribution channel (Google Play) (or whether a particular application does not contain malware, for example), as is the case with the iOS operating system and its distribution channel (App Store).



An example of the above is **Flappy Bird** and its "clones".

This application was developed by Nguyễn Hà Đổng and released for distribution on iOS on 24 May 2013. This application became available for Android OS in 2014, and in January 2014 it became the most downloaded free game. The creator removed the game from the market on 10<sup>th</sup> February 2014. The game recorded more than 50 million downloads.

Already at the time when the original game Flappy Bird was on the market, various clones of this game for the Android OS began to appear, many of which benefited only from the success of the original. However, malware has been deliberately placed in a number of other versions, and it is estimated that up to 79% of clones of this game have been infected with malicious software. [25] Infected clones include, for example, the following products:



Infesting a mobile phone can be one of an attacker's primary targets, as these devices are typically used today for two-factor authentication of Internet banking or shopping. Attackers try to use the information obtained, for example, to withdraw funds by direct access to a user's bank account via the internet banking service or to obtain sensitive information.

### Possibilities of criminal sanctions in the Czech Republic

In the Czech Republic, it is possible to punish an attack with malware according to **Section 230** (Unauthorised access to a computer system and information carrier) of the Criminal Code. **Possession of malware, with the intention to commit a criminal offence** under Section 182 (Violation of the secrecy of transported messages) or a criminal offence under Section 230 of the Criminal Code, **is a criminal offence under Section 231** (Obtaining and possession of access device and computer system passwords and other such data) of the Criminal Code. If the **purpose of a virus** were to obtain, for example, classified information or support from a terrorist group, an attacker could, for example, commit the crimes of **Section 311** (Terrorist attack), **Section 316** (Intelligence) or **Section 317** (Threat of classified information) of the criminal Code **in the preparation stage**.

### Possibilities of criminal sanctions in Poland

Violation of data integrity (viruses, trojans), 268 of the Penal Code, Art. 268a of the Penal Code. This offence concerns, inter alia, stealing personal data, making them available to third parties without the consent of the owner, as well as use them in an unauthorised way. There are financial sanctions (up to PLN 100,000) for committing these acts.

Article 268 Making it difficult for an entitled person to familiarise himself with information

§ 1. Whoever, without being entitled to do so, destroys, damages, deletes or alters a record of important information or in any other way prevents or considerably obstructs an entitled person from learning about it, shall be subject to a fine, the penalty of limitation of liberty or deprivation of liberty for up to 2 years.

§ 2. If the act specified in § 1 concerns a record on a computer data carrier, the perpetrator shall be subject to the penalty of deprivation of liberty for up to 3 years.

§ 3. Whoever, while committing the act specified in § 1 or 2, causes substantial damage to property, shall be subject to the penalty of deprivation of liberty for a term of between 3 months and 5 years.

Article 268a. Destroying, damaging, deleting, altering or impeding access to computer data

§ 1. Whoever, without being entitled to do so, destroys, damages, deletes, alters or obstructs access to computer data or substantially interferes with or prevents the automated processing, storage or transfer of such data

shall be subject to the penalty of deprivation of liberty for up to 3 years.

§ 2. Whoever, while committing the act specified in § 1, causes substantial damage to property,

shall be subject to the penalty of deprivation of liberty for a term of between 3 months and 5 years.

§ 3 The prosecution of the offence specified in § 1 or 2 shall occur on a motion of the injured

### Possibilities of criminal sanctions in Portugal

According to Art. 6(2) of the *Cybercrime Law*, the illegal creation, distribution or dissemination of any computer programme, executable instruction, code or data intended to perform an illegal access to a computer system is penalised as being an Illegal access. The same goes for the crimes of Damage to computer programmes or other computer data [Data interference] (Art. 4(3), Computer sabotage [Illegal interference] (Art. 5(2) and Illegal interception (Art. 7(3), as the Portuguese legislator decided not to have a single provision for the misuse of devices, as the Budapest Convention (Art. 6).

[1] This is not a complete list of different types of malware. Rather, it is about defining the basic types of malware, including an explanation of how they work.

[2] There are companies specialising in "pay per install" (PPI). "PPI then causes plenty of activities leading to the installation of add-ons or other unwanted software, which (in the least harmful case) exchanges ads on websites without the user's knowledge, or inserts them where there are no ads on the site... PPI is based on the fact that those who offer these services do not pay any attention to whether the user wants to install something. They receive up to USD 1.50 per installation, so it's more than certain that fraudulent and automated installations are an essential element of their "business model."

[3] Figure of these pop-ups. For more details see *Adware*. [online]. [cit.10.8.2016]. Available from: <http://www.mhsaoit.com/computer-networking-previous-assignments/324-lesson-16-h-the-secret-history-of-hacking>

[4] [online]. [cit.10.8.2016]. Available from: <https://i.ytimg.com/vi/GcvlB-EpMwA/maxresdefault.jpg>

[5] E.g. an overview of the websites visited, their IP addresses, overviews of installed and used programs, records of downloads of files from the Internet, data on the structure and contents of directories stored on the hard disk, etc.

[6] [cit.8.1.2008]. Available from: <http://www.spyware.cz/go.php?p=spyware&t=clanek&id=9>

[7] These can be, for example: **Browser Helper Object** (DLL library, allowing programmers to change and monitor Internet Explorer); **Hijacker** (software that changes a home page of a web browser); **Dialers** [redirects the telephone line to expensive telephone tariffs (currently mainly attacks on mobile phones and VoIP exchanges)]; **Keystroke Logger / Keylogger** (keystroke monitoring); **Remote Administration** (allows a remote user to control a user's computer system remotely); **Tracer** (a program that monitors the movement of a computer system – typically a mobile device), etc.

[8] For more details see The Malware Museum. *The Malware Museum @ Internet Archive*. [online]. [cit.17.5.2016]. Available from: <https://labsblog.f-secure.com/2016/02/05/the-malware-museum-internet-archive/>

[9] More details e.g. in POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Aleš Čeněk, 2005, p. 216 et seq.

[10] For more details cf. RAK, Roman and Radek KUMMER. *Informační hrozby v letech 2007–2017*. *Security magazín*, 2007, vol. 14, No. 1, p. 4.

[11] Cf. JIROVSKÝ, Václav and Oldřich KRULÍK. *Základní definice vztahující se k tématu*. *Security magazín*, 2007, vol. 14, No. 2, p. 47.

[12] An overview of the most common Trojans, together with a list of their functions and communication ports, can be obtained from various websites available on the Internet. For more details cf. e.g. <http://www.test.bezpecnosti.cz/full.php>

[13] Cf. JIROVSKÝ, Václav. *Kybernetická kriminalita. Nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Prague: Grada, 2007, p. 63.

[14] These programs are sometimes referred to as scanning or scanner programs.

[15] For more details cf. BALIGA, Arati, Liviu IFTODE and Xiaoxin CHEN. *Automated Containment of Rootkits Attacks*. *Computers & Security*, 2008, vol. 27, No. 7–8, pp. 323–334.

[16] Cf. RAK, Roman and Radek KUMMER. *Informační hrozby v letech 2007–2017*. *Security magazín*, 2007, vol. 14, No. 1, p. 5.

[17] E.g. The DNS-Changer Trojan first attacks security programs, removing itself from the list of malicious programs, making it impossible to detect. For more details: PLETZER, Valentin. *Demaskovaný spyware*. *CHIP*, 2007, No. 10, pp. 116–120.

[18] JIROVSKÝ, Václav. *Kybernetická kriminalita. Nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Prague: Grada, 2007, p. 65

[19] Capturing keystrokes and information about running files. [online]. [cit.10.8.2016]. Available from: <http://img.zerosecurity.org/files/2013/10/Keylogger-software-logfile-example.jpg>

[20] [online]. [cit.10.7.2016]. Available from: <https://image.slidesharecdn.com/delljointevent2014november-onur-141105074412-conversion-gate02/95/end-to-end-security-with-palo-alto-networks-onur-kasap-engineer-palo-alto-networks-23-638.jpg?cb=1415174438>

[21] Hyper Text Markup Language – This is the name of the markup language used to create web pages.

[22] Two versions of fake antivirus. [online]. [cit.10.8.2016]. Available from: <http://www.cctsl.com/images/fake-personal-antivirus.jpg>

[23] For more details, see e.g. *Stuxnet*. [online]. [cit.23.7.2016]. Available from: <https://cs.wikipedia.org/wiki/Stuxnet>

[24] *The very first mobile malware: how Kaspersky Lab discovered Cabir*. [online]. [cit.29.6.2015]. Available from: <http://www.kaspersky.com/about/news/virus/2014/The-very-first-mobile-malware-how-Kaspersky-Lab-discovered-Cabir>

See also e.g.:

*Škodlivý kód cílí na mobily, šíří se jako lavina*. [online]. [cit.17.5.2016]. Available from: <https://www.novinky.cz/internet-a-pc/bezpecnost/401956-skodlivy-kod-cili-na-mobily-siri-se-jako-lavina.html>

*Warning! Over 900 Million Android Phones Vulnerable to New „QuadRooter“ Attack*. [online]. [cit.10.8.2016]. Available from: <https://thehackernews.com/2016/08/hack-android-phone.html>

[25] For more details, see e.g. *Flappy Bird Clones Help Mobile Malware Rates Soar*. [online]. [cit.14.8.2016]. Available from: <http://www.mcafee.com/us/security-awareness/articles/flappy-bird-clones.aspx>

## 4.4. Ransomware

The group of malware also includes the so-called extortionate malware, for which the term **ransomware** has been coined [1] (sometimes also referred to as rogueware or scareware). Ransomware is malware that prevents or restricts users from using a computer system properly until an attacker receives a "ransom". Ransomware most often gets on your computer using malware (a Trojan horse or worm) that is located on a website or is an e-mail attachment. Once a malware is safely "established" in a computer system, its own ransomware will be downloaded.

In general, it is possible to distinguish two types of ransomware according to how much they interfere with the actual operation of a computer system. **The first type is ransomware which limits the functionality of an entire computer system** and does not allow a user to use this system at all (e.g. by preventing the operating system from starting or blocking the system screen. A typical example of this type is "Police ransomware" – see below). **The second type is ransomware, which leaves a computer system functional, but locks user data and makes them inaccessible.**

Currently, the second type of ransomware, known as **crypto-ransomware**, is being used. The purpose of this malware is to encrypt a hard disk or selected file types in a computer system, primarily aimed at encrypting a user's private files such as images, text or spreadsheet documents, videos, etc. After encryption, the user usually receives a message that his/her files are encrypted, and if he/she wants to get them back (decrypt), he/she must send a certain amount to the attacker's account. Typically, virtual currencies such as Bitcoin or various prepaid services are used for transactions. In most cases, there is a time limit for payment. After this time, the key that can open the encrypted files is deleted.

### Evolution of ransomware

Ransomware, like any other malware, is evolving, with the first malware to be classified as ransomware appearing around 2005. It was essentially a **fake antivirus (screware)** that, with the help of social engineering, tried to convince a user to pay an amount for cleaning an infected computer system. This ransomware usually allowed a user to use a computer system (it was not locked or data encrypted), but it bothered the user with pop-ups and alerts about non-existent viruses on the computer. This ransomware was very easy to remove.

The massive onset of ransomware can be dated to about 2011, when a ransomware attack blocking access to a Windows user's account began to spread worldwide, announcing that the computer had been blocked by the state's police.

The actual attack consisted in the user becoming infected with malware (typically a "botnet client" was downloaded when visiting some websites [2]) and subsequently became part of a botnet through which its own "**police ransomware**" was distributed. This police ransomware subsequently blocked access to a Windows user account [3] by notifying the user that material infringing the law of the country was found on his/her computer (e.g. copyright infringement, child pornography, etc.). At the same time, the user was invited by the "police" to pay the required amount of money, after which the computer will be unblocked and the whole thing will be "resolved". In this case, the attackers used social engineering techniques, specifically the concerns and trust of a user, and by referring to official authorities, they tried to obtain money from him.

What was striking about the whole case was the fact that a large part of users willingly paid the required amount (in the Czech Republic, this amount ranged between CZK 2000–4000), without verifying whether the real police are authorised to block computers or to "handle" any offences of the user in such a way.

The following print screens show "police ransomware" in various countries and then the versions used in the Czech Republic are shown.



Police ransomware [4]



UK version of police ransomware.[5]

In Europe, various versions (the appearance of the site) of police ransomware gradually appeared. The first version was recorded at the end of 2011, showing the IP address of the connection, the ISP connection and the location [where the IP address of a specific connection provider (ISP) was given], if a user had the webcam turned on, a photo was created and displayed.



Police ransomware – the first version in the Czech Republic

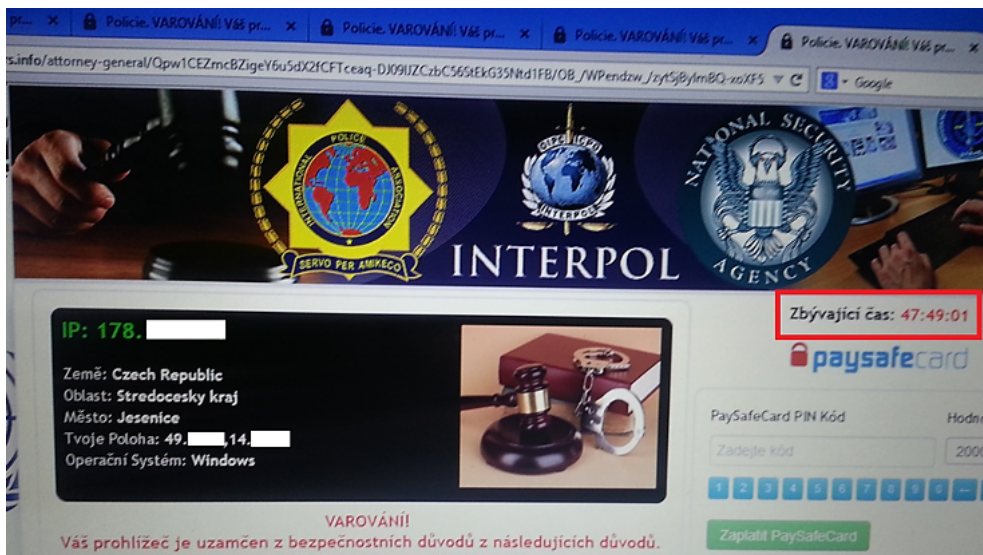
Newer versions, in addition to differing graphically, also displayed the operating system version and username. The Czech language used on the locked page has also been improved.



### Police ransomware in the Czech Republic – other versions

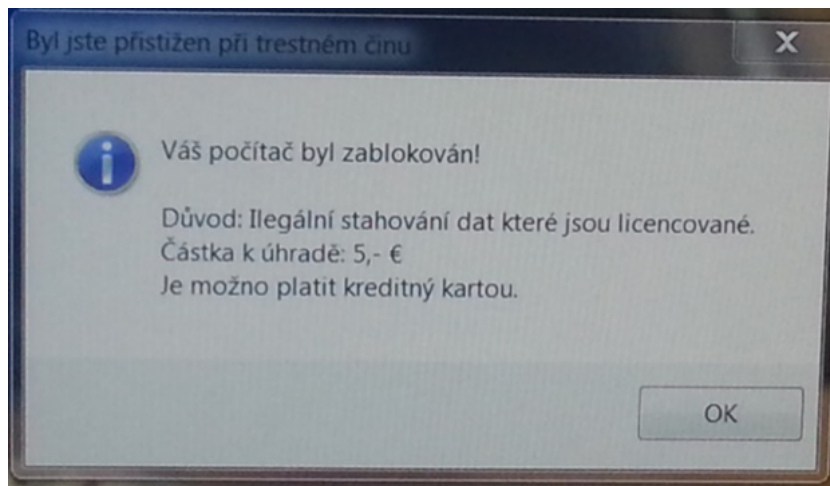
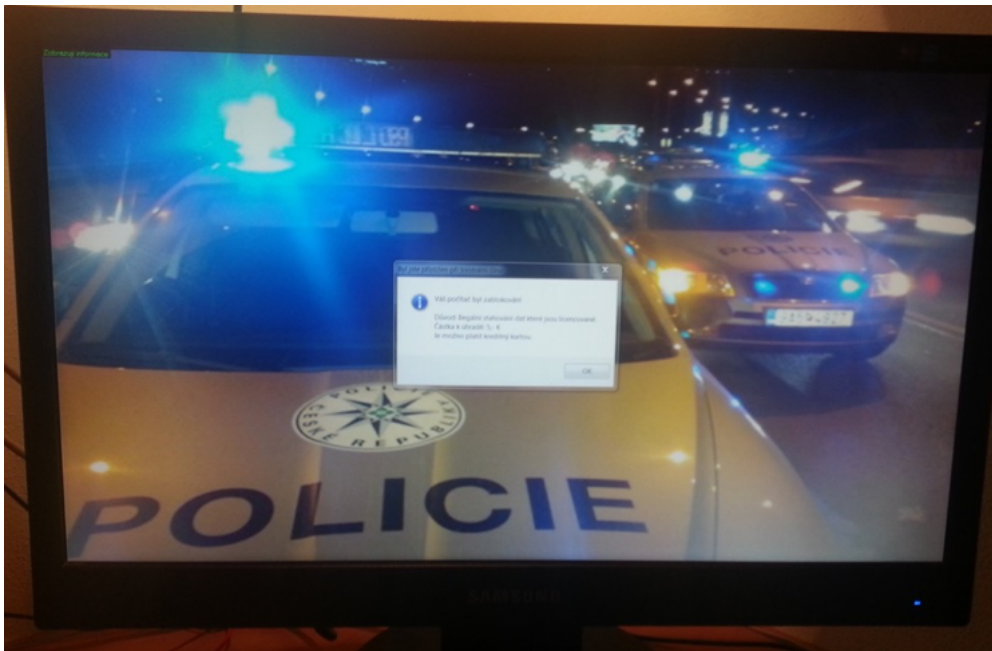
The “police ransomware” described above experienced its greatest expansion in 2011–2013; however, other variants of this malicious software appeared with various modifications later. The following print screens show modifications of the “police ransomware”. Both cases were discovered in 2015. The first print screen shows a ransomware that blocks the dominant web browser used on the infected computer (while other browsers have not been infected). The user was able to use all the functions of the computer system, except for the infected browser.

In addition to the previously mentioned information, the GPS position and the remaining time until payment are displayed.



### Police ransomware in the Czech Republic (2015)

The second print screen shows a “locked” computer, while the ransomware was hidden in the crack of an illegally downloaded and installed game (in this case, it was a Far Cry 4 game downloaded from Czech torrents).



Police ransomware in the Czech Republic (2015)

**Text on the figure:**

*Your computer has been blocked!*

*Reason: Illegal downloading of data that is licensed.*

*Amount to be paid: 5,- €*

*It is possible to pay by credit card.*

Since 2013, there has been a significant change in the case of ransomware. The attackers reduced the attacks which consisted in limiting the functionality of the entire computer system, and primarily focused on locking user data. Data on local disks, disks connected within the computer network and on all connected peripherals (e.g. external USB, HDD, etc.) are locked. Data becomes a "hostage", and breaking encryption is almost impossible. One of the first ransomware of this type was CryptoLocker (then CryptoWall, etc.).

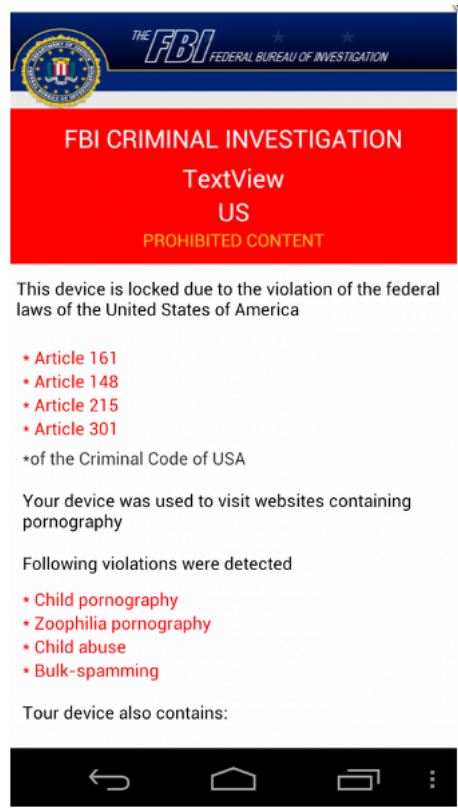




CryptoLocker (2013)



Petya (2017)



### Mobile ransomware (2018)

As part of crime-as-a-service activities, the **ransomware-as-a-service** has been offered since 2016. A user (i.e. an attacker) has the opportunity to define his/her own ransomware according to his ideas. At the same time, he/she is provided with technical background in the form of C&C servers, bitcoin wallets, online 24/7 support, etc. An example of ransomware-as-a-service is the **Ransom32** software.



### Ransomware (client)

Other changes can be observed in attackers' activities. If ransomware is installed, this malware can be targeted, for example, to encrypt stored positions in games, or to "lock" TVs that use the Android operating system. [6]

**Prevention and response to ransomware can be summarised in the following points:**

#### 1. Immediately:

- Avoid interconnecting systems other than necessary
- Prevent communication to the Internet except when necessary
- Change the passwords of privileged accounts

## 2. Within a few days:

- Move backups offline, check the functionality of backups
- Examine business continuity plans and move them out of systems
- Do not delete data about cybersecurity incidents
- Check compromise indicators
- Alert employees to the risk of phishing

## 3. Within a week:

- Verify that backups are separated so that even a privileged administrator cannot delete them
- Prohibit the use of unsigned macros if possible.
- Check network segmentation and control between segments
- Tighten the security policies of end stations (prohibition of running unapproved applications, unsigned PowerShell...)
- If business continuity management is not implemented – develop business continuity plans at least for key systems
- Install antivirus on all relevant devices
- Consider testing and deploying the update

## 4. Long-term recommendations for solving ransomware attacks

- Regular staff training
- Significant network segmentation
- Minimise the use of administrator accounts
- Backup, regularly test backups, keep backups offline
- Rule 3 – 2 – 1 = At least 3 copies on 2 different devices, 1 of which is outside the organisation.
- Have business continuity plans (BCPs) and test them
- Regularly check applications accessible from the Internet and evaluate whether they are still needed

## Possibilities of criminal sanctions in the Czech Republic

In the Czech Republic, it is possible to punish an attack with malware which is ransomware according to **Section 230** (Unauthorised access to a computer system and information carrier) of the Criminal Code. **Possession of malware, with the intention to commit a criminal offence** under Section 182 (Violation of the secrecy of transported messages) or a criminal offence under Section 230 of the Criminal Code, **is a criminal offence under Section 231** (Obtaining and possession of access device and computer system passwords and other such data) of the Criminal Code.

In the case of ransomware, it is also possible to apply the provisions of **Section 230 (3)** of the Criminal Code, where an attacker commits such a criminal offence with the intention of obtaining an unjustified benefit to himself or to another. The application of Section 175 (Blackmailing) of the Criminal Code could also be considered, when a person is forced to pay a given amount by threatening other serious damage (e.g. by being filed with a criminal complaint [\[7\]](#)).

## Possibilities of criminal sanctions in Poland

The laws that apply in Poland are:

Art. 267. Unlawful obtaining of information

Art. 269a. Interference with the operation of an information or data communications system or network

## Possibilities of criminal sanctions in Portugal

As in almost all jurisdictions, ransomware attacks are not specifically criminalised. Though, such actions may be persecuted as Extortions (Art. 223 of the Criminal Code). An alternative, from a strict perspective of Cybercrime, would be Computer-related fraud (Art. 221 of the Criminal), as the its material scope is quite wide, following the wording of the equivalent felony in the text of the *Convention of Budapest* (Art. 8).

Nonetheless, other felonies would also be present, depending on the *modus operandi* of the attackers. Namely, by technical means, being punishable as an Illegal access (Art. 6 of Cybercrime Law), or by *social engineering*, with the inherent Computer-related forgery (Art. 3 of Cybercrime Law).

Furthermore, in itself, the encryption of the victim's data would amount to Computer sabotage [Illegal interference] (Art. 5 of Cybercrime Law), in an aggravated form if critical infrastructures or essential services were disturbed (Art 5(5)(b) of Cybercrime Law).

Finally, if the decryption is not possible, a Damage to computer programmes or other computer data [Data interference] (Art. 4 of Cybercrime Law) would be in place.

---

[1] For example Reventon, CryptoLocker, CryptoWall, Loky, Petya, Cerber, SamSam, JigSawetc. For more details, see e.g.:

Ransomware. [online]. [cit.14.8.2016]. Available from: <https://www.trendmicro.com/vinfo/us/security/definition/ransomware>

[2] Very often it was a site with pornography or other sexual material. A user could also be redirected to these pages from another page with a "bait".

[3] The application was set to "StayOnTop". A user does not see other applications hidden under this "ransom dialog" and is not able to call up the task manager. The Ransomware itself was registered in the Run and RunOnce registers and performed a check every 500 ms, and hid the task manager in the same time range. The only other running application was communication with the C&C server (masked in the browser process).

[4] Police ransomware. [online]. [cit.14.8.2016]. Available from: [https://www.f-secure.com/documents/996508/1018028/multiple\\_ransomware\\_warnings.gif/8d4c9ca2-fc77-433d-ac16-7661ace37f88?t=1409279719000](https://www.f-secure.com/documents/996508/1018028/multiple_ransomware_warnings.gif/8d4c9ca2-fc77-433d-ac16-7661ace37f88?t=1409279719000)

[5] [online]. [cit.14.8.2016]. Available from: [https://sophosnews.files.wordpress.com/2012/11/cool\\_ransom\\_uk\\_full.png](https://sophosnews.files.wordpress.com/2012/11/cool_ransom_uk_full.png)

[6] Cf. for example. *New Ransomware Encrypts Your Game Files*. [online]. [cit.14.8.2016]. Available from: <https://techcrunch.com/2015/03/24/new-ransomware-encrypts-your-game-files/>

*Android Ransomware now targets your Smart TV, Too!* [online]. [cit.14.8.2016]. Available from: <https://thehackernews.com/2016/06/smart-tv-ransomware.html>

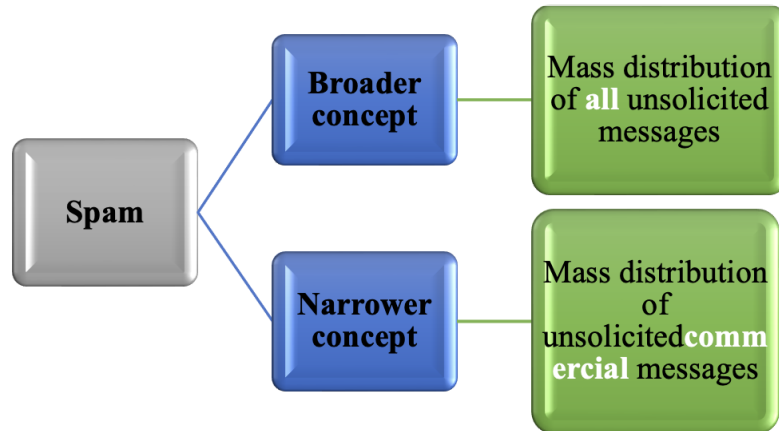
*FLocker Mobile Ransomware Crosses to Smart TV*. [online]. [cit.14.8.2016]. Available from: <http://blog.trendmicro.com/trendlabs-security-intelligence/flocker-ransomware-crosses-smart-tv/>

[7] The concept of other severe damage, see ŠÁMAL, Pavel et al. *Trestnízákoník II. § 140 až 421. (Criminal Code II. Sections 140 to 421). Komentář. (Comment.)* 2nd Edition. Prague: C. H. Beck, 2012, pp. 1752–1753

Specifically, "a threat of other serious damage may consist of a threat of property damage, serious damage to honour or reputation, etc. Another type of serious damage may be the initiation of criminal proceedings as a result of reporting a crime by which the perpetrator threatens the injured party, forcing him to do, neglect or tolerate something. At the same time, it is indecisive whether the injured party has committed a crime, the notification of which he/she is threatened, or not (cf. R 27/1982)."

## 4.5. Spam

From the point of view of information and communication technologies, the content of the term spam can in principle be understood on two levels. In a **narrow sense**, it is the mass dissemination of unsolicited communication, most often of an advertising nature via the Internet, and most often through electronic communication. In a **broad sense**, all unsolicited received messages, i.e. also messages containing viruses, Trojan horses, etc.<sup>[1]</sup> are spam.



Scheme – Division of spams

It is characteristic of spam that it is a **message** that is **sent electronically, in bulk and especially without request**.

Spam uses various communication channels to send unsolicited messages:

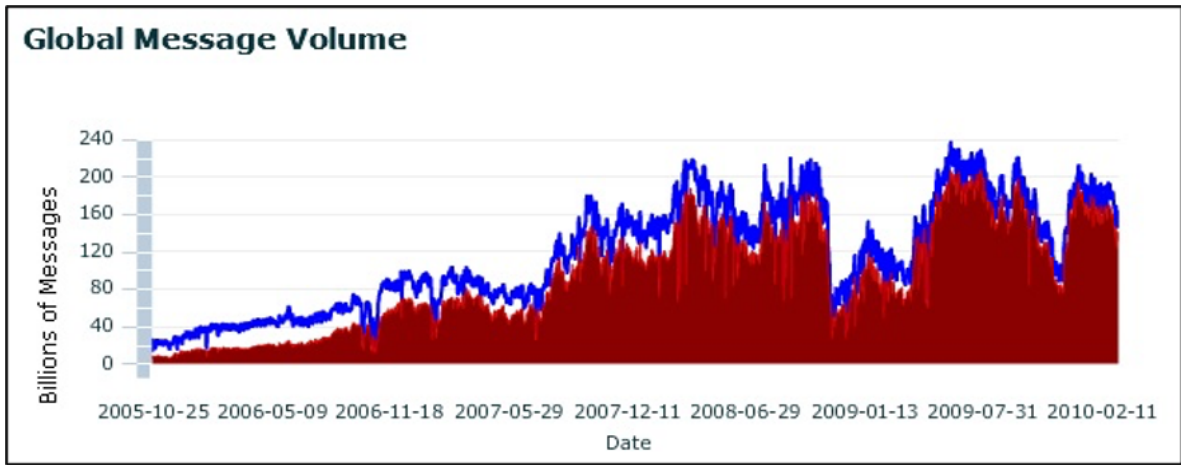
- e-mail;
- othermessenger (ICQ, Skype, etc.);
- SMS, MMS;
- discussion forums, blogs, social networks, etc.;
- gaming platforms, etc.

Spam can contain information:

- **commercial or advertising;**
- **on health and medicine** (This category includes spam offering weight loss products, cosmetics, non-traditional medicine, medicines not available in the region, etc.);
- **financial** (In particular, these are offers of various loans, the possibility of extra income, etc.);
- **pornographic** (This spam either offers various pharmaceuticals to increase sexual potency, or links to sites with pornographic content.);
- **educational** (offers of various courses, trainings, etc.);
- **hoax** (chain letter);
- **political;**
- **religious;**
- **criminal (this category includes messages containing, for example, malware, or linking to sites with malicious code, etc.)**

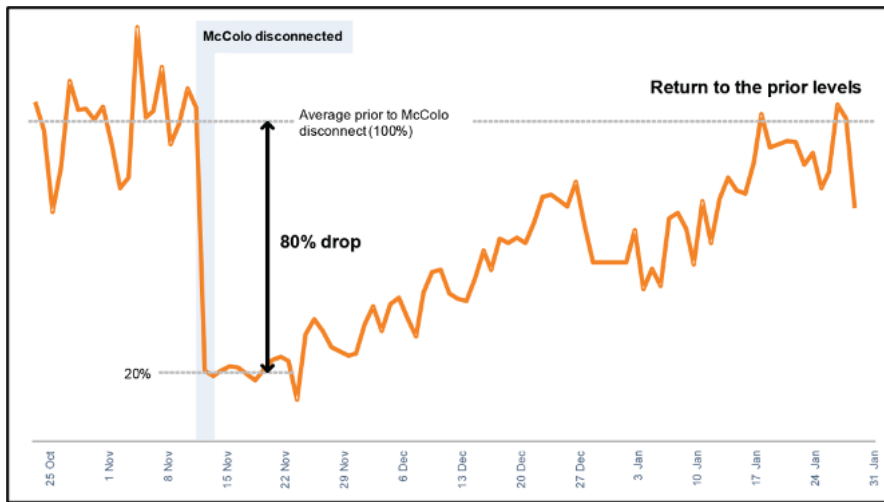
There are currently a large number of statistics showing different numbers of spam in e-mails. For example, Jirovský states that more than 90% of spam in e-mail can be expected. In 2006, an average of 14.5 billion spam messages were sent per day.<sup>[2]</sup> Due to this, many organisations dealing with spam and providing tools to protect against it have emerged. One of these companies was TrustedSource<sup>[3]</sup>, where the following graph comes from. It shows the portion of spam in e-mails from 2005 to 2010. The blue line shows the number of e-mail messages and the red field reflects the number of e-mail spams (both are given in billions).

Regardless of the exact percentages, this type of unsolicited messages currently makes up the majority of all e-mail messages received.<sup>[4]</sup> However, because of a number of technical measures on the part of individual ISPs, the user receives a minimum of messages that represent spam.



Spam development from 2005 to 2010

The significant drop in spam at the end of 2009 is due to the closure of **McColo's** Internet spam business...[5]

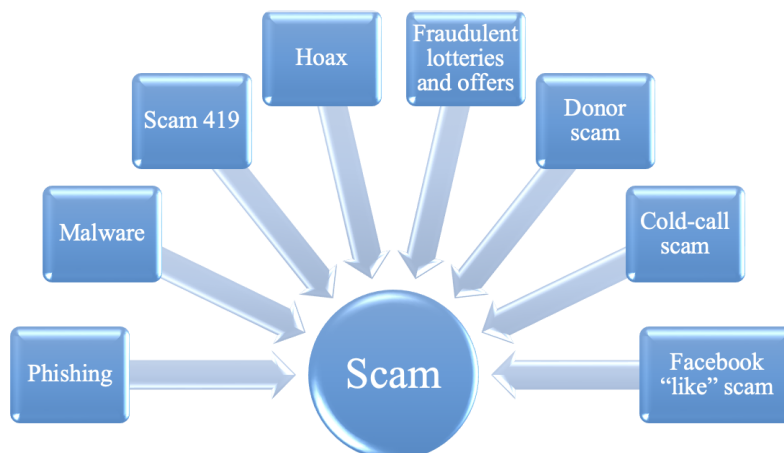


Development of spam after McColo ceased operations in November 2008

Spam interferes with electronic communication, often makes it completely impossible (the information structure is overwhelmed) and thus reduces society's confidence in information technology. However, if spam is restricted, the right to freedom of expression is practically restricted in favour of the right to the protection of personal integrity.

Even for the reason described above, the legal sanction of a spammer is quite complicated and at present the institutes of civil and administrative law are used, as criminal law does not allow to punish a spammer.

Spam containing criminal or other fraudulent content is referred to as **scam**. Scams currently form a significant part of spam and their purpose is, typically using social engineering, to gain a user's trust and force him/her to perform some required actions (e.g. opening an e-mail attachment, visiting the displayed URL, etc.). Scams include *phishing*, *malware*, *419*, *hoax*, *fraudulent lotteries and offers*, *donor scam*, *cold-call scamming*, *Facebook like scam*, etc.



Types of scam scheme

At this point, I will focus primarily on three types of scam, namely **Scam 419**, **Hoax** and **Fraudulent Offers**.

#### 4.5.1. Scam 419

Scam 419 is a designation for e-mails, better known as **Nigerian Letters**. These scams are an example of the transmission of normal crime (fraud) from the real world to the virtual world.

For the sake of interest, we enclose three very different reports having the nature of Scam 419.

##### Report No. 1 – “You have inherited a huge amount of money”

Hi dear,

*I am a lawyer Victoria Josef, I have a message for you concerning my deceased client who bears the same surname as you, I am aware, may not be related to him blood, but is a national in your country who lost his life alongside his immediate family during accident here in Togo engine.*

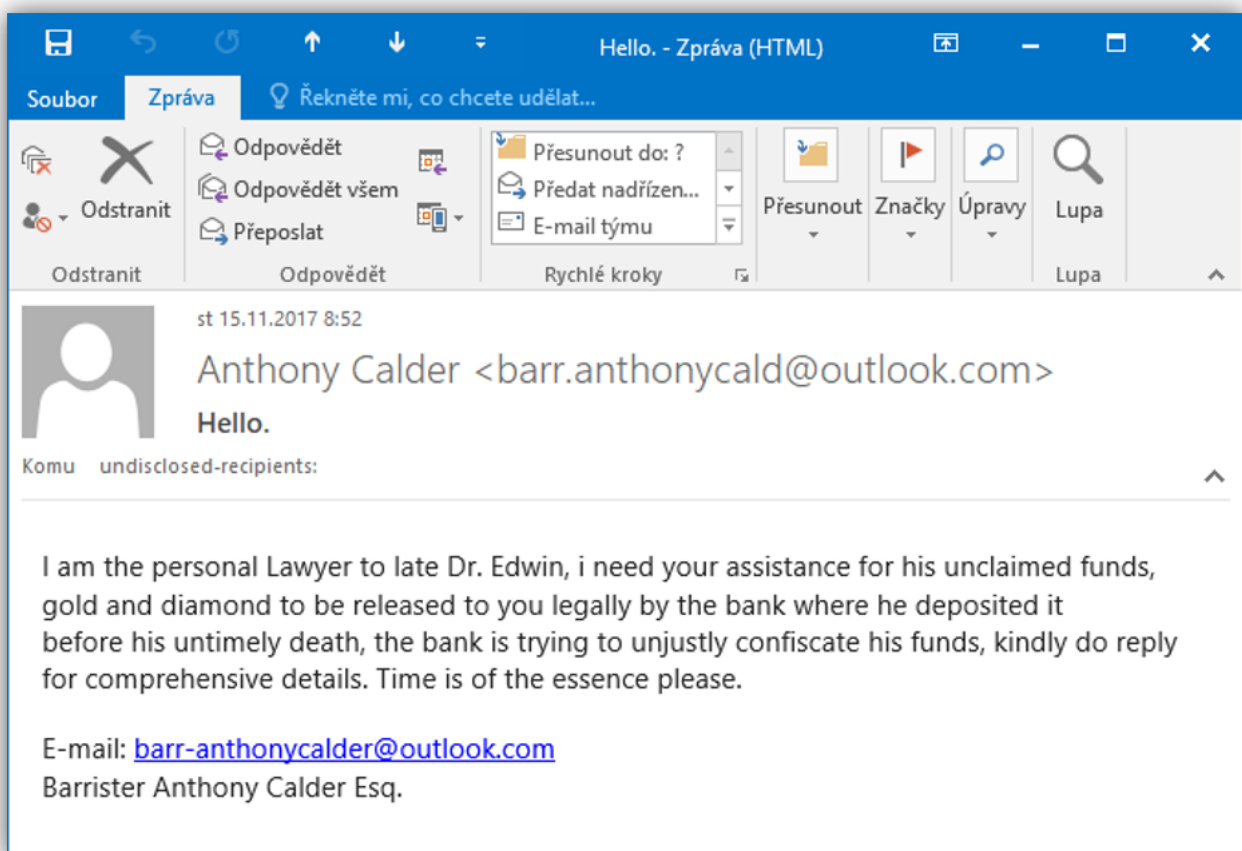
*He left for an amount of \$ 2,700,000, meanwhile, his bank wants to transfer the benefits to one of his extended family members as the presentation can be made through my office. To be honest, this money belongs to my deceased client, who has the same surname and nationality lived with you and worked here in Togo for more than 20 years as a contractor, but died in a fatal car accident along with all members of his family in 2009 and recently, the bank where this money is stored gave me a mandate to provide some member of his family to demand this money or else it will be passed to the government treasury account as abandoned money.*

*I don't want that to happen, but the problem is that his supposed closest relatives died in this same car accident and all his efforts to trace his family members since his death have been unsuccessful in disputing when he never introduced some of them to me while he was alive.*

*Friend, that's why I embarked on this mission to find someone to work from hand to hand with me claiming this fund to help our families and the needy, instead of allowing these corrupt government officials to take over this hard-earned money, just like that and scatter it, leaving the poor masses to suffer. For me to pick up on you among the millions of people on Facebook; Just mean it's God who made our way upset, so let's work together with one mind as we share the money the way he claimed it.*

*Please indicate your interest in this statement so that I can provide you with regard to work and guidelines.*

Attorney Victoria Joseph Esq.



##### Message No. 2 – “I fell in love”

Hello Darling,

*My name is Joe Anita I'm a woman, I found out his identity on the side, and I want to learn that we know more about each other and share social life with culture, and I have nothing to say, so please reply me, so I send my data to you and I will say more about myself in my paintings. Thank you very much.*

Your joy Anita



ne 05.06.2016 21:29

MojzeszlgAnselm@gmail.com

You love sports and girls wish to meet a man.

Komu MojzeszlgAnselm@gmail.com

V této zprávě byly odebrány nadbytečné konce řádků.



hfriirj3hfk.jpg  
23 KB

Hi, my name is Narmina I'm a girl from Azerbaijan. Azerbaijan It's an independent country, you can find it on maps.  
I find your address in dating marriage agency. This service is in our town. This is a dating agency has many connections with most online dating sites, and they have a common list of the forms and e-mail addresses. I come to this agency, pay some money and they give me your e-mail address.  
So I very much hope that you will answer my letter soon.  
I'm very interesting, soft and tender girl. But I'm very lonely in my life. I want to find good man for serious relations.  
I'm ready to spend all my life with such man! I hope you like my picture, I send you with this letter.  
And if you still free from serious relations, just let me know and send the answer, may be it's our chance to escape from loneliness.  
I would like to see yours picture also, and find out more about you.  
Looking forward for your answer.  
Narmina

Message No. 3 – "Instant sex"

Desperate for a F\*ckbuddy - Zprá...

Soubor Zpráva Řekněte mi, co chcete udělat...

Odpovědět Odpovědět všem Předat nadřízen... Předat nadřízen... E-mail týmu Přesunout Značky Úpravy Lupa

Odstranit Odpovědět Odpovědět všem Předat nadřízen... Předat nadřízen... E-mail týmu Přesunout Značky Úpravy Lupa

Odstranit Odpovědět Rychlé kroky Lupa

pá 15.07.2016 16:01

Bryony Roark <Roark\_Jayda@e.amexpub.com>  
Desperate for a F\*ckbuddy

i'm so hungry for s\*x that i will do anything for it!  
you can just f\*ck me and leave, i dont mind ;)  
r u ready? my wet pu\*\*y is waiting...  
my username is SkankiS1ut7, lo0k at my n3w plcs [\\*\\*\\*here\\*\\*\\*](#)





## 5 engines detected this URL

URL <http://6url.ru/iWTI>  
Host [6url.ru](http://6url.ru)   
Downloaded file [c0b6418dce31ded4e3408dc1d7857ca315f0197804ba94780b87084381062168](#)   
Last analysis 2016-07-11 08:35:44 UTC  
Community score **-7**

5 / 68

Detection	Details	Community
Avira	Malware	BitDefender  Phishing
CLEAN MX	Phishing	Dr.Web  Malicious
Fortinet	Malware	Websense ThreatSeeker  Suspicious
ADMINUSLabs	Clean	AegisLab WebGuard  Clean
AlienVault	Clean	Antiy-AVL  Clean

### Message No. 4 – A Nigerian astronaut has been forgotten in space and needs to get home

The news began to spread in 2004, at which time the “first African astronaut” had been in space for 14 years without a break. It should be noted that the length of his stay surpassed all the times of astronauts (perhaps in total). I received the last version of this Scam 419 in 2016. Although I am very sorry for this imaginary astronaut (26 years in space and alone), I certainly do not intend to contribute to fraudsters. Unfortunately, despite the completely meaningless content and unsubstantiated information contained in this e-mail, there are a large number of people who want to help a person in need (thanks to this help, this scam could be included in the *donor scam* group).

**Subject: Nigerian Astronaut Wants To Come Home**  
**Dr. Bakare Tunde**  
**Astronautics Project Manager**  
**National Space Research and Development Agency (NASRDA)**  
**Plot 555**  
**Misau Street**  
**PMB 437**  
**Garki, Abuja, FCT NIGERIA**

Dear Mr. Sir,

**REQUEST FOR ASSISTANCE-STRICTLY CONFIDENTIAL**

I am Dr. Bakare Tunde, the cousin of Nigerian Astronaut, Air Force Major Abacha Tunde. He was the first African in space when he made a secret flight to the Salyut 6 space station in 1979. He was on a later Soviet spaceflight, Soyuz T-16Z to the secret Soviet military space station Salyut 8T in 1989. He was stranded there in 1990 when the Soviet Union was dissolved. His other Soviet crew members returned to earth on the Soyuz T-16Z, but his place was taken up by return cargo. There have been occasional Progrez supply flights to keep him going since that time. He is in good humor, but wants to come home.

In the 14-years since he has been on the station, he has accumulated flight pay and interest amounting to almost \$ 15,000,000 American Dollars. This is held in a trust at the Lagos National Savings and Trust Association. If we can obtain access to this money, we can place a down payment with the Russian Space Authorities for a Soyuz return flight to bring him back to Earth. I am told this will cost \$ 3,000,000 American Dollars. In order to access the his trust fund we need your assistance.

Consequently, my colleagues and I are willing to transfer the total amount to your account or subsequent disbursement, since we as civil servants are prohibited by the Code of Conduct Bureau (Civil Service Laws) from opening and/ or operating foreign accounts in our names.

Needless to say, the trust reposed on you at this juncture is enormous. In return, we have agreed to offer you 20 percent of the transferred sum, while 10 percent shall be set aside for incidental expenses (internal and external) between the parties in the course of the transaction. You will be mandated to remit the balance 70 percent to other accounts in due course.

Kindly expedite action as we are behind schedule to enable us include downpayment in this financial quarter.

Please acknowledge the receipt of this message via my direct number 234 (0) 9-234-2220 only.

Yours Sincerely, Dr. Bakare Tunde  
Astronautics Project Manager  
tip@nasrda.gov.ng

<http://www.nasrda.gov.ng/>

Due to the nature of fraud, it would be possible, in some cases, to label or subordinate Scam 419 to acts having the nature of phishing.

#### 4.5.2. Hoax

A hoax (a fiction, prank, press canard) is another form of spam or scam. The label "hoax" is used for chain messages (such as: "*pass it on*", "*if you don't send it to 20 other people... happens.*", etc.), which contain distorted, untrue, misleading or other false information. A hoax often contains warnings about attacks, descriptions of dangers, pleas for help, calls, petitions, statements of celebrities, chain letters of happiness, funny messages, pictures and videos in presentations, playing cats and other animals, etc.

#### 4.5.3. Fraudulent offers

A very successful form of scam is various fraudulent offers, which can be sent in bulk or in a targeted manner. At present, such offers are sent not only via e-mails, but also via any instant messengers, social networks, auction portals, etc.

With regard to the **mass distribution** of fraudulent offers, it is possible to imagine a number of activities on the principle of "pyramid" or "plane", offers of advantageous work from home [6], "guaranteed" methods of value for money (with the highest interest rates), offers on loan (with the lowest interest rates), "great" job opportunities, etc.

**Targeted sending** of fraudulent offers should also include conduct that is not merely spam, but is, for example, a combination of bidding on a specific type of goods within auction portals and subsequent communication with users who have accepted this bid. These are so-called "auction frauds".

**NAJRYCHLEJŠIE RASTÚCE PODNIKANIE Z DOMOVA VO SVETE!**

**POĎTE NA PREHĽADKU ZADARMO!**

**PÁČILO BY SA VÁM ZARÁBAŤ VIAC AKO 8.847,00 \$ ZA MESIAC PRÁCOU Z DOMU?**

**PRÁVE TERAZ MÁTE PRÍSTUP ZADARMO!**

Stačí vyplniť krátky formulár na tejto strane a môžete sa vydať na cestu k finančnej stabilite

MENO

PRIEZVISKO

TELEFÓN

E-MAIL

POTVRTE

STIFORP CZECH

TISÍCE OBYČAJNÝCH LUDÍ SI ZARÁJ SLUŠNÉ ŽIVOBÝTÍ... DĽAJŠOU

#### Irresistible offer of work from home (mass distribution within the social network Facebook)

At present, it is certainly no longer the rule that bulk or targeted offers are written in suspicious or broken Czech (or are written in English or Russian), on the contrary, an attacker's effort is to convince a victim of absolute correctness, seriousness and "honesty" of his actions. Auction portals very often fraudulently offer various types of electronics, especially mobile phones and computers. The actual fraud can then consist, for example, of changing essential information [e.g. country of origin of the mobile phone; information that it is a copy (forgery) of the phone] or non-delivery of the goods as such. (The attacker very often requests payment of the full amount or advance.)

The imaginativeness of the attackers is considerable in the Internet environment, and in the case of any offers, advertisements, and especially the sending of advances or payments, it is advisable to be paranoid and not trust unknown persons.

In the case of fraudulent offers, where an attacker tries to obtain various advances or other payments in advance, such conduct can be punished according to **Section 209** (Fraud) of the Criminal Code.

#### Possibilities of criminal sanctions in the Czech Republic

**As far as the criminal sanction of spam and spammers is concerned, it is currently not fully (re)solved in the Czech Republic.** There is no national or international legal protection against this undesirable behaviour. Even the Convention on Cybercrime does not include the definition of spam as a criminal offence.

For example, in the **USA**, spammers [7] have been convicted of sending spam in the past. For example, **Jeremy Jaynes** was sentenced in 2007 by a Virginia court to 9 years in prison. He was accused in 2003, as evidenced by 53,000 spams sent within three days. However, the prosecutor said he believed Jaynes was responsible for sending more than 10,000,000 spams a day, which should have earned him approximately \$ 750,000 a month.

Due to the fact that only one form of harmful conduct cannot be included under the term spamming, it is very difficult to punish spamming under criminal law. This can only be done for its individual types. In certain cases, it is possible to punish the collection of e-mail addresses if such collection meets the objective elements of the criminal offence of unauthorised handling of personal data under **Section 180** (Unauthorised handling of personal data) of the Criminal Code. If the spam contains malware or is intended to commit fraud, it is possible to punish a spammer's activities according to the provisions relating to malware or phishing.

#### Possibilities of criminal sanctions in Poland

In Poland sending unsolicited commercial information by electronic means of communication is considered an offence and is subject to a fine. This is regulated by the Act of 18 July 2002 on the provision of electronic services (Journal of Laws of 2002 No. 144, item1204):

Art. 24. 1. Whoever sends, by means of electronic communication, unsolicited commercial information, shall be subject to the penalty of a fine.

(2) The prosecution of the offence, referred to in section 1, shall occur at the request of the injured party.

Article 25 Adjudication in cases related to the offences specified in Articles 23 and 24 shall be conducted pursuant to the provisions on proceedings in petty offence cases.

## Possibilities of criminal sanctions in Portugal

Also in Portugal, in general terms, spamming itself is not considered as a criminal offence. However, following Art. 14(1)(f)(g)(h)(i)(j) of Law No. 41/2004, on data protection and privacy in electronic communications, spammers for commercial purposes must pay administrative fines, from a minimum of € 1500 to a maximum of € 5000000.

However, as an exception, being the content of messages within the scope of Law No. 52/2003, on the fight against terrorism, it might be considered as a criminal offence (Arts. 2 and 4).

---

[1] To classify spam, cf. for example GONZÁLES-TALAVÁN, Guillermo. A Simple, Configurable SMTP Anti-spam Filter: Greylists. *Computers & Security*, 2006, vol. 25, No. 3, pp. 229–236.

[2] Cf. for example: *Spam statistics*. [online]. [cit.14.8.2016]. Available from: <https://www.spamcop.net/spamstats.shtml>

*Spam Statistics and Facts*. [online]. [cit.14.8.2016]. Available from: <http://www.spamlaws.com/spam-stats.html>

[3] Original online source: <http://www.trustedsource.org/TS?do=homehttp://spam-filter-review.toptenreviews.com/spam-statistics.html> [cit.12.2.2010].

[4] It is not possible to determine exactly what percentage of all e-mails are spam. The different sources available give different, sometimes very different numbers. E.g. One of the providers of antispam solutions, POSTINI, recorded in March 2005 within 24 hours that 10 out of 12 e-mails were spam. The frequency of sending spam, cf. e.g. LANCE, James. *Phishing bez záhad*. Prague: Grada, 2007, p. 22, SCHRYEN, Guido. The Impact that Placing Email Addresses on the Internet Has on the Receipt of Spam: An Empirical Analysis. *Computers & Security*, 2007, vol. 26, No. 5, pp. 361–372.

[5] *Malware, mayhem, and the McColo takedown*. [online]. [cit.14.8.2016]. Available from: <http://betanews.com/2008/11/13/malware-mayhem-and-the-mccolo-takedown/>

[6] On the one hand, these offers may consist of a request such as: "send us \$10 to our account and we will send you instructions on how to earn \$8,847 a month." The second possibility is that these job offers do not require any fee in advance, they only require user registration. By registering, an attacker receives personal data about a user. An e-mail from this company, containing e.g. malware, etc., can then be sent to the user's e-mail address.

[7] *Convicted spammer challenging Va. law* [online]. [cit.14.8.2016]. Available from: [http://www.usatoday.com/tech/news/techpolicy/2007-09-12-spammer-va\\_N.htm](http://www.usatoday.com/tech/news/techpolicy/2007-09-12-spammer-va_N.htm)

*Top Spammer Sentenced to Nearly Four Years*. [online]. [cit.14.8.2016]. Available from: <http://www.pcworld.com/article/148780/spam.html>

*Buffalo Spammer jde na 7 let za mříže kvůli rozesílání nevyžádané pošty*. [online]. [cit.14.8.2016]. Available from: [http://technet.idnes.cz/buffalo-spammer-jde-na-7-let-za-mrize-kvuli-rozesilani-nevyzadane-posty-13i-/tec\\_reportaze.aspx?c=A040528\\_28629\\_tec\\_aktuality](http://technet.idnes.cz/buffalo-spammer-jde-na-7-let-za-mrize-kvuli-rozesilani-nevyzadane-posty-13i-/tec_reportaze.aspx?c=A040528_28629_tec_aktuality)

## 4.6. Phishing, Pharming, Spear Phishing, Vishing, Smishing

### 4.6.1. Phishing

The term phishing is most often referred to as fraudulent or deceptive conduct, the aim of which is to obtain information about a user, such as username, password, credit card number, PIN, etc.

In a **narrow sense**, phishing is an action that requires a user to visit a fraudulent site (displaying, for example, an internet banking website, online store, etc.) and then fill in "login information", or this information is required directly (e.g. when filling out a form, etc.).

In a **broad sense**, phishing can be defined as any fraudulent conduct that is intended to inspire confidence in a user, reduce his/her vigilance or otherwise force him/her to accept a scenario prepared in advance by an attacker. In this broad sense, the user is no longer required to fill in the data, but is provided with a message (or the user is redirected to a page) typically containing malware that collects the data. Furthermore, donor scams, etc. can be included in this broader sense.

In both cases, a user who is the target of a phishing attack is deceived. The difference lies mainly in the degree of interaction required of the user.

Phishing in essence is the use of social engineering. Phishing can also be done in the real world (see scams, etc.), but the virtual world allows an attacker to send fraudulent messages to a huge number of potential victims with minimal effort. Phishing can, with a great deal of exaggeration, be compared to "*carpet bombing*". As with bombing, phishing it targets a relatively unspecified number of victims so that an attacker has hope of success. For example, in 2014, Google stated that a scam with really good phishing have 45% success rate in gaining user data.[\[1\]](#)

Phishing is not just about e-mails. It is possible to find phishing within instant messages (Skype, ICQ, Jabber, etc.), social networks, SMS and MMS messages, chat rooms, scams (fraudulent offers of job or goods, etc.), fake browser applications[\[2\]](#), etc.

#### **Phishing in a narrow sense**

The principle of a "*classic*" phishing attack most often consists in sending a so-called phishing e-mail to an injured party, which at first glance does not raise any suspicion that it should be a fraudulent message. Such an e-mail usually includes a link that a user is prompted to click.

After clicking on the attached link, the user gets to a fraudulent website, which is almost impossible to distinguish in terms of appearance and function from the original correct web box. If it is an imitation of a website, through which it is possible to make payments, access secure accounts, manage such accounts, etc., then the data entered by the user are automatically sent to the attacker.[\[3\]](#) In this way, the attacker can obtain identification data of users of Internet banking services, access to individual bank accounts of users of infected systems, identification numbers and other data on payment cards with the help of which it is then possible to make payments in the Internet environment, etc.

An actual phishing attack takes place in several steps.[\[4\]](#)

#### **1. Planning of a phishing attack**

In this phase of a phishing attack, a target (user group) is selected and the method to be used for the attack is selected. What type of technical security the target uses is assessed, what are the risks of the attacker revealing his identity, etc.

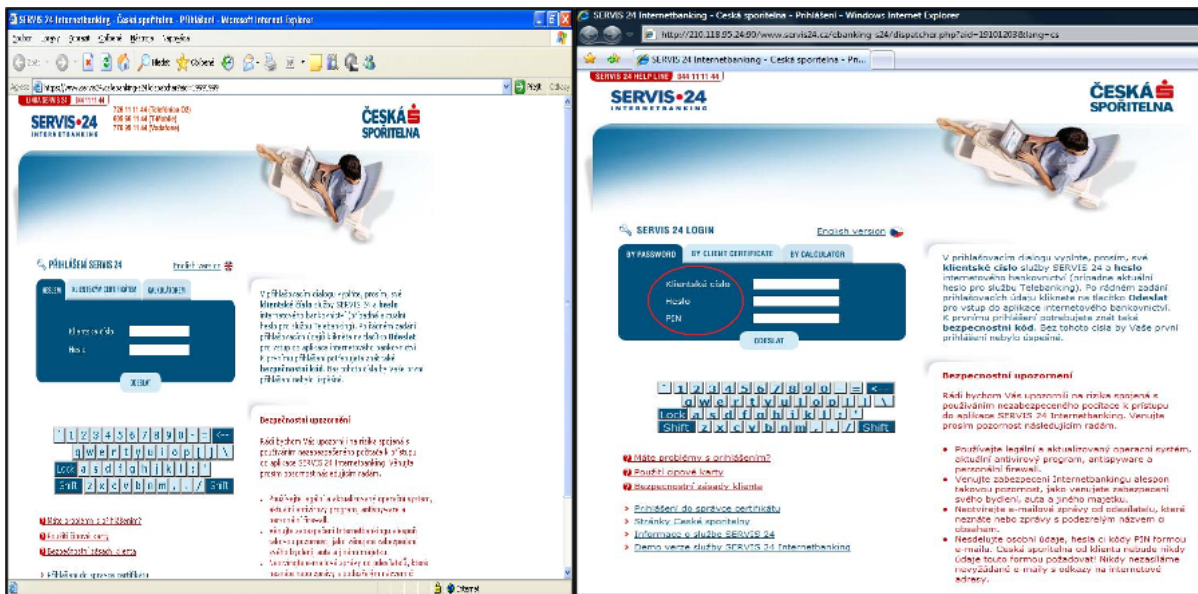
#### **2. Creating conditions for a phishing attack**

At this stage, a technical solution to a phishing attack is taking place. An attacker obtains lists of e-mail addresses of users to whom a phishing e-mail is to be sent, a data box is created, where the system sends the acquired user data, a trusted message is created, which is then distributed to users.

#### **3. Phishing attack**

A phishing e-mail is delivered to individual users and, depending on the quality of processing of this e-mail and other factors (user experience, user's awareness of phishing issues, anti-phishing software of the target, etc.), the data is sent to the attacker's data box. In this phase of a phishing attack, the user encounters a phishing e-mail for the first time.

As a pretext, information about a bug in the company's security system or another warning is often used, which should make the user trust the authenticity of this message. After activating the interactive link, the person is redirected to a website created by the attacker, faithfully copying the original page of the financial institution. The user is prompted to fill in login details, usually including the card number and PIN code. The completed data is sent to the address of the phisher, who then draws some or all of the funds from the account and thus causes a loss to the client (see the following figure).



Original page (left) and fraudulent page (right)

#### 4. Data collection

The attacker obtains data that was entered by individual users of the compromised system in a fake website environment.

#### 5. Withdrawal of funds or other profits from a phishing attack

Using the obtained data, the attacker enters the actual bank accounts of individual users and withdraws funds. By transferring to other, especially foreign accounts, diluting these funds and using other techniques, the withdrawn funds become virtually untraceable.

It is very difficult to determine how many phishing attacks are carried out worldwide each day. It is also problematic to determine how many clients of compromised companies respond to a phishing e-mail. The rate of return is estimated to be between 0.01 and 0.1%.

Forecasts in 2007 estimated that "classic" phishing scams or campaigns would increase in the future. [5] These forecasts have been fulfilled in part, as the number of "classic" phishing campaigns is declining, but phishing in a broad sense is on the rise [6], especially its new modifications or linking phishing with other types of attacks (malware, botnet, etc.).

#### Phishing in a broad sense

As part of demonstrating phishing in a broad sense, I will present four campaigns that took place in the Czech Republic and were more or less successful. Of course, these attacks are not the only phishing attacks in a broad sense that took place in the Czech Republic. The reason for choosing these four specific attacks is the fact that I want to point out in particular the innovative approach of the attacker and the appropriate combination of technical attack with social engineering. Specifically, the attacks are:

1. Debt/Bank/Execution
2. Czech Post (Česká pošta)
3. Christmas and gifts
4. Seznam.cz – One Time Password

##### 4.6.1.1. Debt/Bank/Execution [7]

A phishing campaign professionally called DBE hit the Czech Republic on a massive scale in 2014 (with the reverberations of this campaign lasting at least until the end of 2015). The attack itself was very precisely prepared and included both a phishing and a distribution of malware (to computers and mobile devices). The whole attack can be divided into the following phases:

1. Phishing campaign
2. Installation of malware to a computer
3. Access to online banking
4. Installation of malware to a mobile device
5. Transfer and withdrawal of funds

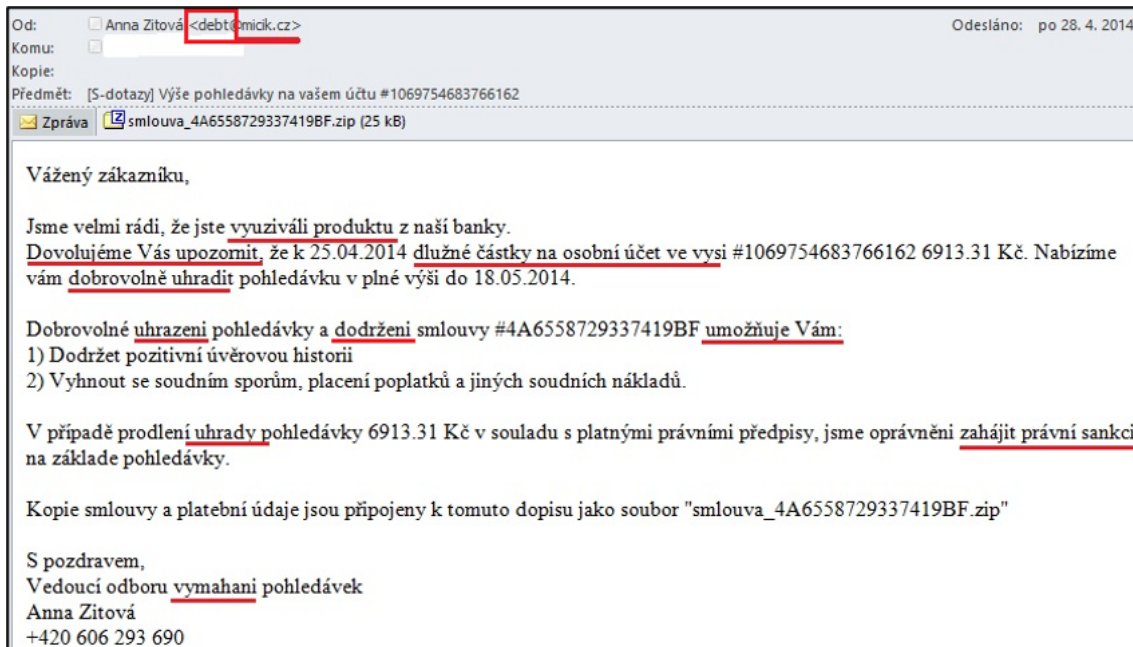
##### Ad 1) Phishing campaign

The first prerequisite for attackers to be able to successfully obtain money was a large phishing campaign to which a sufficient number of people would respond. The actual distribution of fraudulent e-mails has been broken down into three successive waves of phishing messages:

- I. **Debt** (debt@...); March–April 2014
- II. **Bank** (bank@...); May–June 2014
- III. **Execution** (emissions@...); July–September 2014

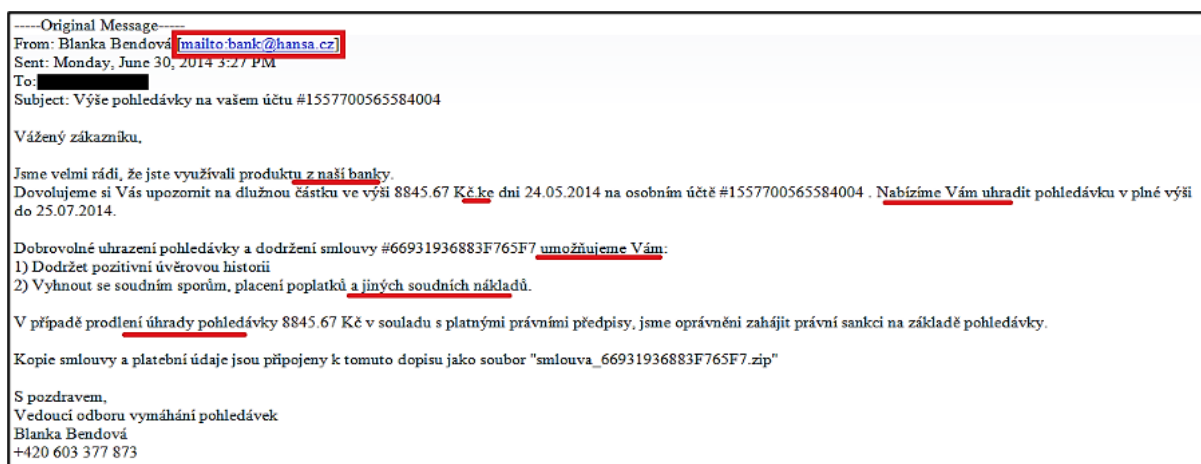
Within the individual campaigns, there was an increase in the “quality” of their own e-mail messages and, in particular, a better use of social engineering in relation to the presumed victims in the target region, i.e. the Czech Republic. However, all of the above phishing campaigns had at least two features in common. First, it was the fact that the attachment in the sent e-mail always contained a file that looked like a text document but was an executable file, specifically malware: Trojan.[8]. The second common feature was that social engineering took advantage of the concerns of the addressed individuals from possible litigation, in the latter case from execution.

The first wave of phishing attacks used very bad Czech. It was sent out from various, not entirely trusted domains when it comes to debt collection, registered in the Czech Republic (e.g. [micik.cz](http://micik.cz) or [dhome.cz](http://dhome.cz) etc.). Various names of persons and existing telephone numbers were used, traceable on the Internet (the person owning this number ultimately had nothing to do with the attack).



Fraudulent e-mail sent as part of the Debt wave

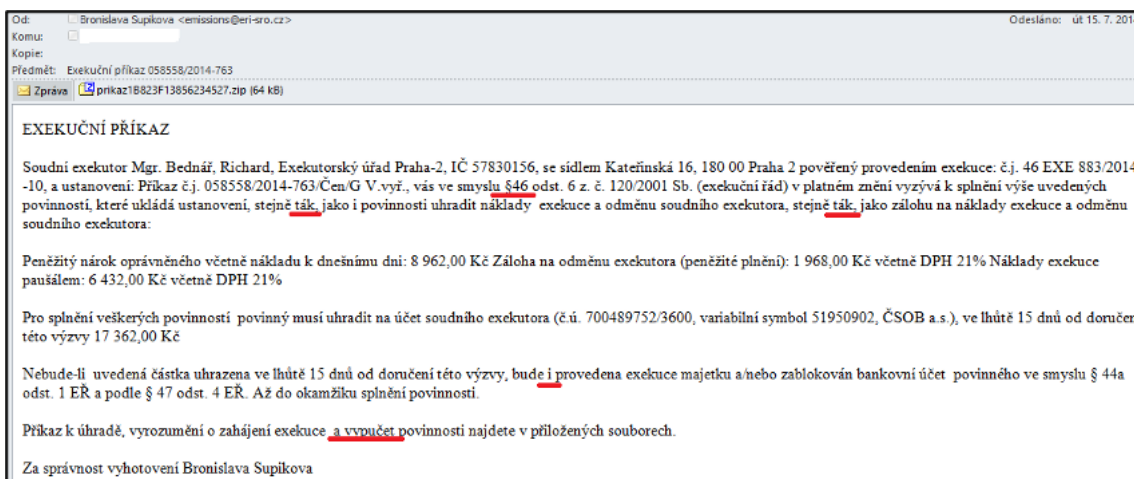
In the second wave, the Czech language used improved.



Fraudulent e-mail sent as part of the Bank wave

At the time these phishing attacks began to appear, various security organisations and CSIRT teams [9], as well as mass media, published warnings including instructions on how to handle such reports. [10].

Both campaigns were relatively successful, but the most successful was the attack where the fraudulent e-mail was a warning (call) from an executor.



### Fraudulent e-mail sent as part of the Execution wave

The Czech language used in the “execution order” especially contained errors in use of diacritics, or some sentences were formulated in a less than natural style. (The most obvious errors are underlined.) However, the names of real executors were used, traceable on the Internet (said executor had nothing to do with the attack), as well as the real-looking numbers of executions.

#### Ad2) Installation of malware to a computer

As mentioned earlier, all phishing campaigns included malware in the attachment of the sent e-mail: TrojanDownloader (i.e. malware designed to download other malware). This malware was primarily created and targeted at the Windows XP operating system, which was discontinued in March 2014.

Název	Velikost
smlouva_26.06.2013-signed_893589F59975811EF.exe	85 504

Executable file (malware) contained in the attachment to the fraudulent e-mails

After running the attachment, “Tinba” malware (bank Trojan horse) was installed, which was downloaded from the Internet in the background, while a contract or an execution order in a text editor was shown to a user. [11]

The malware was written to the directory: **Users/specific user/AppData/Roaming/brothel**. In this directory, it was possible to find `ate.exe`, which is a file that was created after opening the executable file in the phishing e-mail. At the same time, an appropriate key was created in the registry in the **HKEY\_CURRENT\_USERSoftwareMicrosoftWindowsCurrentVersionRun** branch. In this way, it was possible to verify whether this was malware resulting from this attack.

#### Ad3) Access to online banking

The next step of the attacker was to wait for the moment when the victim logs in to online banking. The malware on the computer is able to record communication between the user and online banking, and an attacker has the ability to monitor this communication. The user barely had a chance to detect the attack because the URL in the browser belonged to the bank and the communication was secure (HTTPS).

*“The actual theft of sensitive data takes place by inserting malicious code into the official websites of banks. Configuration scripts are downloaded from C&C servers (machines belonging to attackers, used to control the botnet) and decrypted as described above. What is interesting is the reuse of the same format of configuration files of the well-known bank Trojans Carberp and Spyeye. For each botuid (a unique value that identifies the user's environment), a list of usernames and passwords is stored on the C&C server. Additional scripts are downloaded depending on the bank used, either `hXXps://andry-shop.com/gate/get_html.js`; `hXXps://andry-shop.com/csob/gate/get_html.js`; or `hXXps://yourfashionstore.net/panel/a5kGcvBqtV`, which will be downloaded if the victim visits the websites of Česká spořitelna, ČSOB, or Fia.” [12]*

#### Ad 4) Installation of malware to a mobile device

The next step of the attacker was to convince users of the need to increase security when accessing online banking. The reason for the warning issued by the alleged bank (actually an attacker-controlled website) was to “increase” the security of the connection. The victim was offered a page with a choice of mobile device operating systems (Android, Windows Phone, Blackberry and iPhone OS), but only the Android version allowed the download of malware to the phone. The attackers chose various ways of distributing malware to a phone, from simply sending an SMS message with a link from which a user was meant to download the program, to sending an SMS message and a QR code. [13]

### The text of the message:

CS-S24

Download a security from

Bit.ly/Tp9JjU




The malware downloaded and installed on the mobile device was detected by Avast! as Android: *Perkele-T*.

**Vážení kliente!**

SMS byla odeslána na číslo: +. Doručení SMS do 5 minut.

Pokud Vám nepřišel SMS, naskenujte QR kód



Je třeba nainstalovat aplikace OTPdirekt. Stiskněte tlačítko "Zobrazit instrukce".

**Zobrazit instrukce**

**Pozor! Nemůžete pokračovat dale bez OTP hesla.**

OTP heslo:  **Pokračovat**

#### Downloading malware to the phone

The purpose of this malware was to gain access and full control over the secondary authentication means (two-factor authentication), which in most cases is the mobile phone. If a user was using an operating system other than Android, they received a message: *"Please try again later."*

#### Ad5) Transfer and withdrawal of funds

The next step of the attacker was to draw funds from the attacked account and sent them to the account of white horses, who were then to withdraw cash or transfer it to other accounts. Due to full control (using malware) of both Internet banking access data (see infected computer) and control of the secondary authentication device (see infected mobile phone – when authentication messages were forwarded to the attacker without being seen by the victim), the attacker could enter a "legitimate" money transfer order.

According to a report from Avast!, Russian-speaking attackers were behind this attack. SMS messages from the infected phone were forwarded to the number 79023501934, which was registered in the Astrakhan region, Russia. [\[14\]](#)

#### 4.6.1.2. Czech Post (Česká pošta)

The second major phishing attack began in November 2014 and continued until December 2014. At the beginning of the attack, there was a phishing e-mail with a "Czech Post" (Česká pošta) notification that you were not found as the addressee of a shipment and that you should download the shipment information. The Czech language used in this phishing e-mail is one of the worst you can come across in phishing. Apparently one of the automatic translators from the Internet was used to generate this e-mail.

The fraudulent e-mails were sent from addresses that do not belong to Czech Post. These were, for example, addresses: [upport@cs-post.net](mailto:upport@cs-post.net), [tracktrace@cs-post.net](mailto:tracktrace@cs-post.net), [cpost@cs-post.net](mailto:cpost@cs-post.net), [post@cs-post.net](mailto:post@cs-post.net), [zasilka@cs-post.net](mailto:zasilka@cs-post.net), which due to the domain **cs-post** could arouse a user's belief that this is a Czech Post site. However, it should be noted that **cs-post** was registered in the **.net** domain, while the actual pages of the Czech Post (Česká pošta) are registered in the **.cz** domain (see <https://www.ceskaposta.cz>).

Česká pošta (post@cs-post.info)  
Jan Mráček Informace o Vaší zásilce  
Dnes 18. 11. 2014, 11:21:28



Jan Mráček

Vaše zásilka **DR490714563C** dorazila na 14. listopadu 2014. Courier nebyl schopen doručit zásilku pro vás. Vytisknout informace o Vaší zásilky a ukázat, že v nejbližší poště, aby si zásilku.

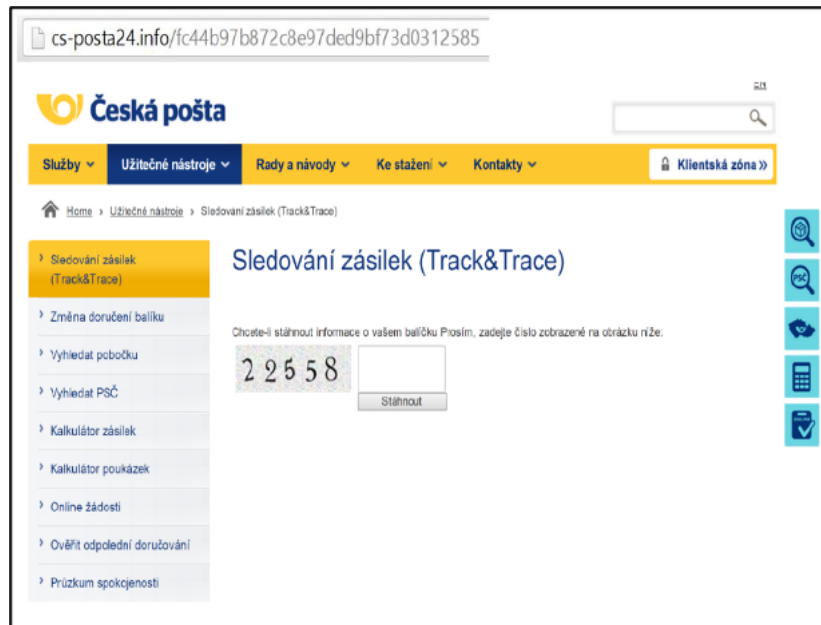
[Stáhněte si informace o zásilka](#)

Pokud je zásilka neobdrží do 15 pracovních dnů Česká pošta bude mít právo nárokovat odškodnění od si pro své udržení ve výši 52,5 Kč za každý den vedení. Můžete si najít informace o postupu a podmínkách při pozemku chov v nejbližší kanceláři.

Toto je generován automaticky zprávu, pokud nechcete přijímat zprávy od nás prosím [odhlásit](#)

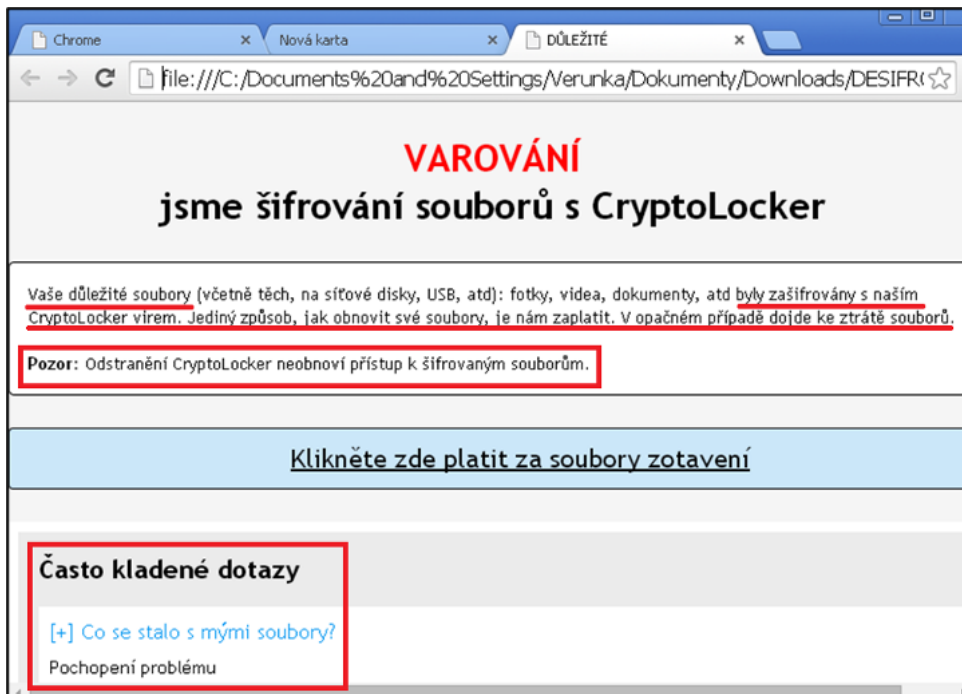
#### Fraudulent e-mail from "Česká pošta"

If a user clicked on the box: *Download information about the shipment*, he/she was redirected to pages that resembled the actual pages of the Czech Post (Českápošta). Here, a user was asked to enter a security code (Captcha) and was then allowed to download a .zip file that contained "tracked shipment information". As in the previous phishing campaign, an executable file (ransomware) was stored in the attachment, but the purpose was to encrypt a user's data.



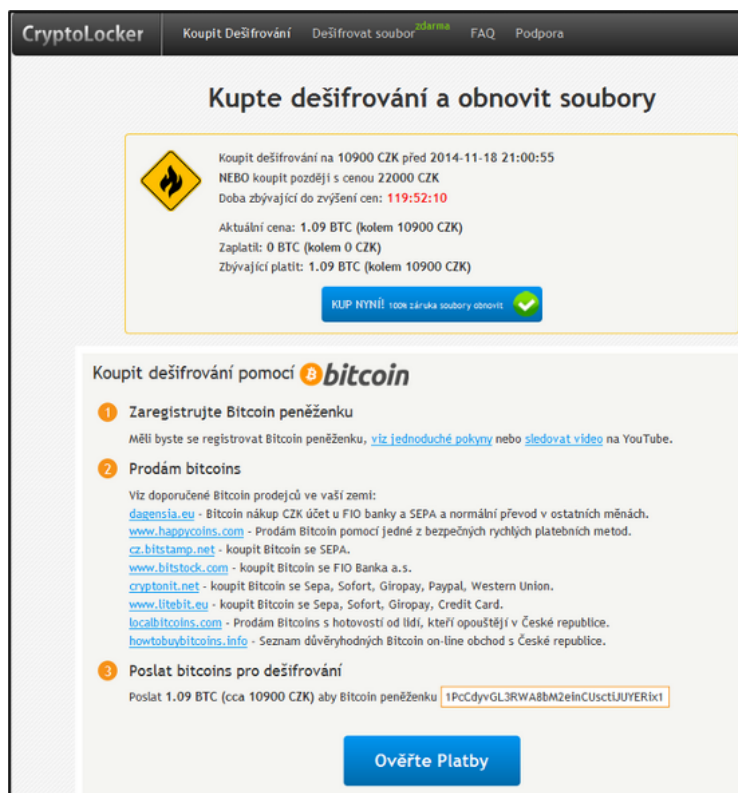
#### Fraudulent site of the "Czech Post" (Českápošta)"

After encrypting the data, a user was prompted to pay for a key that was able to decrypt the encrypted files. The prompt has already been written in a much better version of Czech. The user could also learn some answers to some questions that may have bothered him/her.



Information that was displayed to the user after encrypting his/her data

Data recovery at that time cost 1.09 BTC, and in addition to the conversion to Czech crowns, the user was shown detailed instructions on how to set up a bitcoin wallet, where and how to buy bitcoins and where to send them.



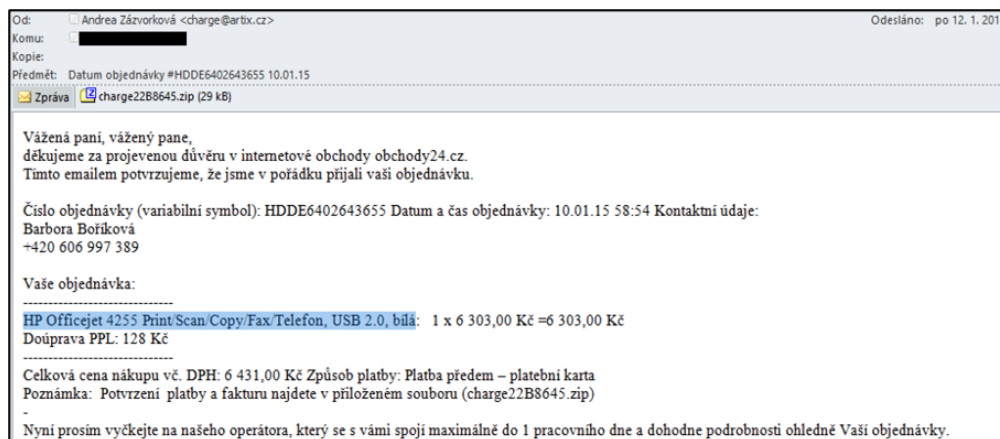
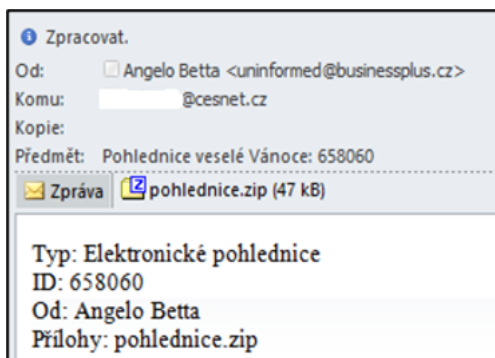
Instructions on how to decrypt your files [15]

The attack is specific in that it added ransomware to a phishing campaign, which immediately began encrypting a user's data, and in that a pre-Christmas period was used to carry out the attack, in which many people wait for shipments to be delivered. Due to these two factors, the attack was very successful.

#### 4.6.1.3. Christmas and gifts

Another major phishing attack began during December 2014 (specifically during the Christmas period) and continued in January 2015. This attack was divided into two phases. In the first phase, users were sent e-mail wishes with a Merry Christmas via an electronic postcard. In the second phase, messages confirming an order for electronics were sent during January. The message informed a user that he/she had purchased goods (e.g. printer, hard drive, camera, etc.) for which he/she had paid in advance with a payment card, referring to the invoice in the attachment.

Both attacks have a common element, which is the malware contained in an e-mail attachment. Specifically, it was a Trojan horse (*Kryptik*), which was presented as a screen saver. This malware was, as in the case of the attack mentioned in chap. 4.6.1.1 Debt/Bank/Execution compressed in a .zip file. After unpacking the .zip file, many users did not consider the .scr\_[16].file to be executable and thus infected their own computer.



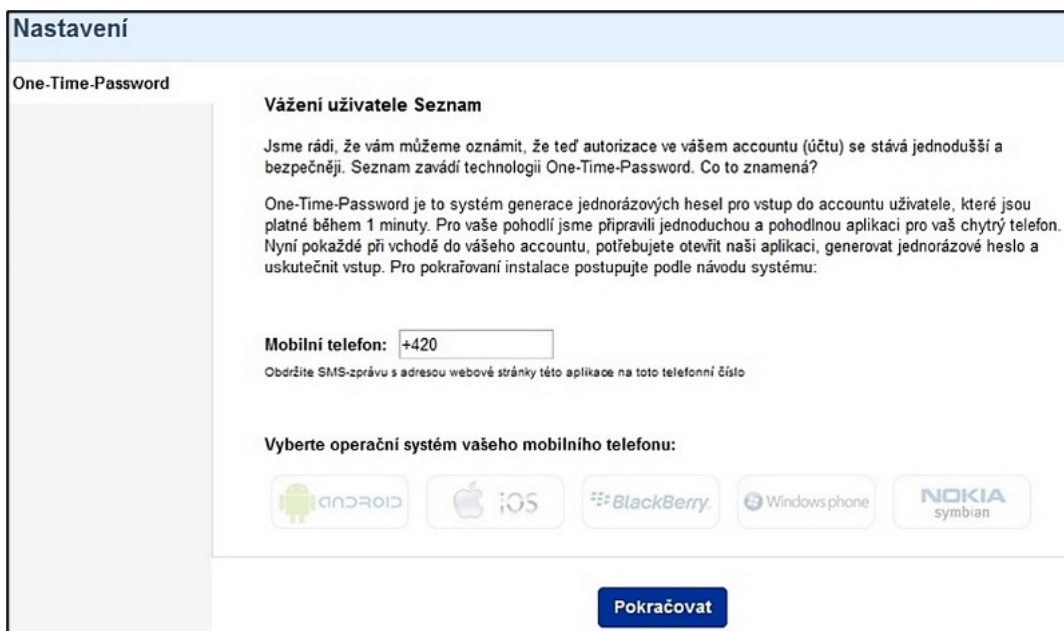
#### Samples of postcard and shop phishing messages

The attack is specific in that it used a type of file that many users do not consider dangerous, and the timing of the attack. Thanks to various chain e-mails, users have become accustomed to opening electronic postcards or attachments that look like this, without more thorough checking of the content. The second attack was planned so that a user check if he/she had not actually ordered any goods that were not delivered to him/her due to the Christmas holidays.

#### 4.6.1.4. Seznam.cz – One Time Password

The latest phishing attack demonstrates a significant change in attackers' tactics. An attacker still takes advantage of the fact that malware has infected a computer. An attacker can control this computer himself or rent it out, for example, as part of a botnet. The actual infection could have occurred, for example, through another incoming e-mail, when visiting infected sites, or otherwise. The attacker's goal in the case of Seznam – One Time Password [17] was to gain control of the user's mobile phone.

The malware that was installed on a computer prompted a user to log in to the Seznam.cz e-mail box to install a tool for easier and safer work with their mailbox on their mobile phone. A user is then guided step by step through installing the SeznamOTP application from an untrusted source. At the end of the installation, a user is provided with his/her "unique licence key". In reality, however, a user has installed malware on his/her mobile phone.



Welcome screen of SeznamOTP installation.[18]

The **risk** of this last phishing attack is that the “**phishing message**” was not delivered via e-mail or other means of communication, but was **displayed to a user only in a specific situation** (in this case after logging in to the seznam.cz mailbox) and the **initiator of this message was malware found on an already infected computer**. The **second risk factor is the fact that the security request is not linked to a bank account**. Therefore, a user may not be aware of the dangers of installing this application.

In the Czech Republic, it is possible to punish conduct that has the nature of “classical phishing” according to **Section 209** (Fraud) of the Criminal Code. The fraud is completed by enrichment. A creation of a replica of a website and the acquisition of login names and passwords could then be qualified as a preparation or attempt of a criminal offence according to Section 209 of the Criminal Code. Obtaining access data, including account numbers, payment card numbers and PIN codes without their further use, will not be a criminal offence.

#### Possibilities of criminal sanctions in the Czech Republic

In the case of combined forms of phishing attacks, where malware is used to infect a computer, such conduct of an offender must also be punished in accordance with **Section 230** (Unauthorised access to the computer system and information carrier) of the Criminal Code. If the aim of the phishing attack is to gain an unjustified benefit for oneself or another, it is also possible to apply the provisions of **Section 230 (3)** of the Criminal Code.

In specific cases, it would be possible to use the provisions of **Section 234** (Unauthorised measures, counterfeiting and alteration of the means of payment) of the Criminal Code.

#### Possibilities of criminal sanctions in Poland

Breach of the secret of communication (sniffing) - art. 267 § 3 of the Penal Code. This type of crime consists in obtaining proprietary information, e.g. through sniffers, i.e. programs that intercept data (passwords and user IDs). Such an act is punishable by up to 2 years imprisonment.

Article 267 Unlawful obtaining of information

§ 1. Whoever, without authorisation, gains access to information not intended for him, by opening a closed letter, connecting to a telecommunications network or breaking or bypassing an electronic, magnetic, IT or other specific protection thereof, shall be subject to a fine, the penalty of limitation of liberty or deprivation of liberty for up to 2 years.

§ 2. The same punishment shall be imposed on anyone, who without authorisation, gains access to the whole or any part of an information system.

§ 3. The same punishment shall be imposed on anyone, who in order to obtain information to which he is not entitled, establishes or uses an eavesdropping or visual device, or other device or software.

§ 4. The same punishment shall be imposed on anyone, who discloses information obtained in the manner specified in § 1-3 to another person.

§ 5. The prosecution of the offence specified in § 1-4 shall occur on the motion of the injured person.

#### Possibilities of criminal sanctions in Portugal

Being the dissemination of malware criminalised (Art. 6(2) of the Cybercrime Law), as mentioned, in itself, the creation of inauthentic data would be considered an offence as Computer-related forgery (Art. 3 of the Cybercrime). Besides, if the purpose of such creation has a fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person, on the expenses of the victim, it would also be considered a Computer-related fraud (Art. 221(1) of the Criminal Code).

In addition, the counterfeiting of cards and other non-cash means of payment, including the misuse of devices, is punished as aggravated offences (Art. 3-A to 3-F of the Cybercrime Law).

On the other hand, being within the scope of Law No. 52/2003, on the fight against terrorism, computer-related forgery and computer-related fraud would be considered as aggravated offences.

#### 4.6.2. Pharming

**Pharming**<sup>[19]</sup> is a more sophisticated and dangerous form of phishing. This is an attack on a DNS (Domain Name System) server, which translates a domain name into an IP address. The attack occurs when a user enters an address of a web server he/she wants to access in an Internet browser. However, it will not link to the appropriate IP address of the original web server, but to a different, spoofed IP address. Websites at a fake address usually very faithfully imitate the original pages. They are practically indistinguishable from them. A user then enters his/her credentials that an attacker obtains. This attack is usually carried out when a user accesses Internet banking sites.

*"Fake websites can be used to install viruses or Trojan horses on a user's computer, or they can be used by attackers to try to obtain personal or financial information, which can then be misused to steal identity. Pharming is a particularly dangerous form of cybercrime, because in the case of an infected DNS server, a user can become a victim even if no malware is installed on their computer at all. Even if you use precautionary measures, such as entering Internet addresses manually or using only trusted bookmarks, you are not protected against this type of attack, because unwanted redirection only occurs after the computer sends a connection request."* <sup>[20]</sup>

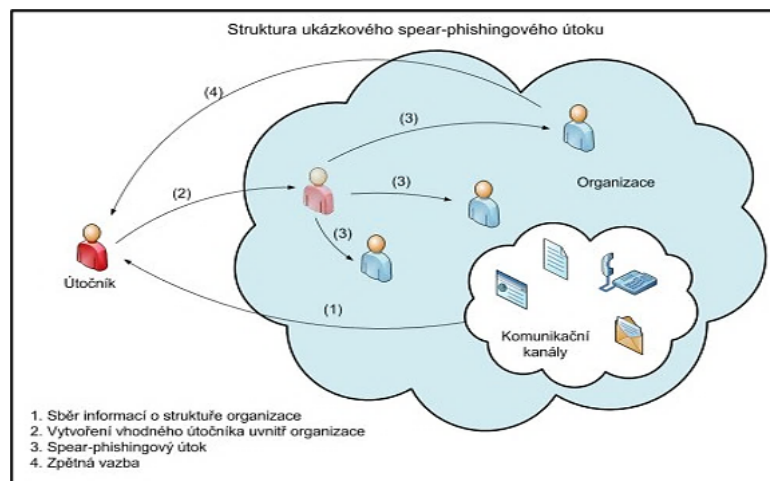
The other typical way of pharming is to attack an end user's computer with malware, where a lower level of security can be expected. This malware changes the hosts file to divert traffic from the intended destination and redirect users to a fake website.

Criminal sanctions are similar to those in the case of phishing. The same according to Portuguese and Polish law.

#### 4.6.3. Spear Phishing

Spear phishing is one of the forms of phishing attack, but with the difference that spear phishing is a precisely targeted attack, unlike phishing, which is a rather widespread (random) attack. The target of an attack is usually a specific group, organisation or individual, specifically information and data contained in this organisation (e.g. intellectual property, personal and financial data, business strategies, classified information, etc.).

The difference between spear phishing and classic phishing is in who is the sender of the messages in question. At the beginning of an attack, it is the attacker who uses open sources to find out as much information as possible about the attacked organisation, its structure, etc. He also creates a high-quality e-mail or other message and begins to communicate with a person from within the organisation as a colleague. The attacker will then use this person as a means of spreading other messages (e.g. infected malware) within the organisation. As the person who is "known" to the victims, he has no problem communicating with the victims, who verifies the attacker's messages less, if at all.<sup>[21]</sup>



Structure of a spear-phishing attack<sup>[22]</sup>

Text on the figure:

*The structure of a sample spear-phishing attack*

*Attacker – Organisation – Communication channels*

*1. Collection of information about the structure of an organisation*

*2. Creating a suitable attacker within the organisation*

*3. Spear-phishing attack*

*4. Feedback*



The course of a spear phishing attack [23].

### Possibilities of criminal sanctions in the Czech Republic

A spear phisher's punishment is similar to that of phishing. For example, a terrorist organisation may be behind a spear phishing attack. In this case, liability for a criminal offence under **Section 311** (Terrorist attack) of the Criminal Code is not ruled out.

### Possibilities of criminal sanctions in Poland

The same laws apply as those for phishing.

### Possibilities of criminal sanctions in Portugal

The conclusion being the same as for phishing in general, including those related to terrorism.

### 4.6.4. Vishing

The term vishing [24] refers to telephone phishing, in which an attacker uses a social engineering technique and tries to lure sensitive information from a user (e.g. account numbers, login details – name and password, payment card numbers, etc.). The attacker is deliberately trying to falsify his/her identity. Attackers often present themselves as representatives of real banks or other institutions in order to arouse as little suspicion as possible in a user. Vishing is used in VoIP (Voice over Internet Protocol) telephony.

### 4.6.5. Smishing

Smishing [25] works on a similar principle as vishing or phishing, but uses SMS messages to distribute messages. As part of smishing, it is primarily an attempt to force a user to pay an amount (for example, call a toll-free line, send a donor SMS, etc.) or click on suspicious URL links. If a user visits the URL, he/she is redirected to a page that exploits certain vulnerabilities in the computer system, or the user is prompted for sensitive information or malware. [26]

Example of smishing:

"Warning – this is automatically generated message from (local bank name), your credit card has been blocked. To reactivate, call 866 ### ##"

### Possibilities of criminal sanctions in the Czech Republic

Criminal sanctions of vishing and smishing are similar to those in the case of phishing.

### Possibilities of criminal sanctions in Poland

The same laws apply as those for phishing.

### Possibilities of criminal sanctions in Portugal

Also in this case, the conclusions regarding criminalisation is the same as for phishing in general, including those related to terrorism.

[1] See e.g. *Google says the best phishing scams have a 45-percent success rate*. [online]. [cit. 14.8.2016]. Available from: <https://www.engadget.com/2014/11/08/google-says-the-best-phishing-scams-have-a-45-percent-success-r/>

*Phishing by the Numbers: Must-Know Phishing Statistics 2016*. [online]. [cit. 14.8.2016]. Available from: <https://blog.barkly.com/phishing-statistics-2016>

[2] See e.g. *Beware of Fake Android Prisma Apps Running Phishing, Malware Scam* [online]. [cit.14.8.2016]. Available from: <https://www.hackread.com/fake-android-prisma-app-phishing-malware/>

[3] LANCE, James. *Phishing bez záhad*. Prague: Grada Publishing, 2007. p. 45.

[4] WILSON Tracy, V. *How Phishing Works*. [online]. [cit.14.8.2016]. Available from: <http://computer.howstuffworks.com/phishing.htm>

[5] The development trends of phishing – see also e.g. DODGE, Ronald. C., Curtis CARVE and Aaron J. FERGUSON. *Phishing for User Security Awareness*. *Computers & Security*, 2007, vol. 26, No. 1, pp. 73–80.

[6] **According to the following study, phishing has increased by 250% in the last 6 months**. See *Phishing Activity Trends Report*. [online]. [cit.14.8.2016]. Available from: [https://docs.apwg.org/reports/apwg\\_trends\\_report\\_q1\\_2016.pdf](https://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf)

[7] Hereinafter referred to as **DBE**.

[8] For more details see results from VirusTotal. [online]. [cit. 15.8.2016]. Available from:

<https://www.virustotal.com/cs/file/62170532b1f656c6917fa66d0ed98462e106f3aa139273c9f2c3a370a67d265f/analysis/1471330723/>

[9] Computer Security Incident Response Team. For more details, see e.g.: <https://www.csirt.cz/>

[10] See e.g. *Pozor na zprávu o údajné neuhrazené pohledávce - jedná se o podvod*. [online]. [cit.15.8.2016]. Available from:

<https://www.csirt.cz/page/2073/pozor-na-zpravu-o-udajne-neuhrazene-pohledavce---jedna-se-o-podvod/>

*Znovu se objevily podvodné zprávy*. [online]. [cit.15.8.2016]. Available from: <https://www.csirt.cz/news/security/?page=97>

*PODVODNÉ EMAILY hrozí exekucí, nic neplatte a neotvírejte!* [online]. [cit.15.8.2016]. Available from:

<http://tn.nova.cz/clanek/zpravy/cernakronika/podvodne-emaily-hrozi-exekuci-nic-jim-neplatte-a-neotvirejte.html>

*Pozor na zprávu o výzvě k úhradě před exekucí - jedná se o podvod*. [online]. [cit.15.8.2016]. Available from: <https://www.csirt.cz/news/security/?page=87>

*Čo sa skrýva v prílohe podvodných e-mailov?* [online]. [cit.15.8.2016]. Available from: <https://blog.nic.cz/2014/07/23/co-sa-skriva-v-prilohe-podvodnych-e-mailov-2/>

[11] For more details see the analysis of Tinba malware functionality: *W32. Tinba (Tinybanker)*. [online]. [cit.15.8.2016]. Available from: [https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp\\_w32-tinba-tinybanker.pdf](https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_w32-tinba-tinybanker.pdf)

[12] HOŘEJŠÍ, Jaromír. *Falešný exekuční příkaz ohrožuje uživatele českých bank*. [online]. [cit.15.8.2016]. Available from:

<https://blog.avast.com/cs/2014/07/17/falesny-exekucni-prikaz-ohrozuje-uzivatele-ceskych-bank-2/>

[13] Ibid. – image with captcha code.

[14] HOŘEJŠÍ, Jaromír. *Falešný exekuční příkaz ohrožuje uživatele českých bank*. [online]. [cit.15.8.2016]. Available from:

<https://blog.avast.com/cs/2014/07/17/falesny-exekucni-prikaz-ohrozuje-uzivatele-ceskych-bank-2/>

[15] *Sledování zásilky České pošty aneb nová havěť*. [online]. [cit.14.8.2016]. Available from: <http://www.viry.cz/sledovani-zasilky-ceske-posty-aneb-nova-havet/>

[16] SCR files are executable files.

*They are primarily assigned with the Unknown Apple II File program (found on Golden Orchard Apple II CD Rom). The following are also assigned: Windows Screen Saver, Image Pro Plus Ver. 1.x - 4.5.1.x Macro (Media Cybernetics Inc.), TrialDirector Script File (inData Corporation), Screen Dump, Screen Font, Statistica Scrollsheet, Procomm Plus Screen Snapshot File, Movie Master Screenplay, Mastercam Dialog Script File (CNC Software Inc.), Sun Raster Graphic, LocoScript Screen Font File (LocoScript Software), Faxview Fax, DOS DEBUG Input File, Script a FileViewPro.*

*Co znamená přípona souboru SCR*. [online]. [cit.14.8.2016]. Available from: <http://www.solvusoft.com/cs/file-extensions/file-extension-scr/>

[17] Hereinafter referred to as the **SeznamOTP**

[18] More information about this malware and the course of the entire attack can be found, for example, at: *Podvodníci mění taktiku. Našlínovou cestu, jak vybilít lidem účty*. [online]. [cit.14.8.2016]. Available from: <https://www.novinky.cz/internet-a-pc/bezpecnost/364094-podvodnici-meni-taktiku-naslinovou-cestu-jak-vybilit-lidem-ucty.html>

[19] It is a combination of words **farming** and **phreaking**.

[20] For more details see *Co je pharming?* [online]. [cit.14.8.2016]. Available from: <http://www.kaspersky.com/cz/internet-security-center/definitions/pharming>

[21] *"An attacker chooses an organisation working with valuable information, analyses the website to obtain information about the personnel structure, employees and procedures (for more detailed information about employees, such an attacker can use their private pages and discussion forums) and in the next step, the attacker creates a report whose content, form and appearance mimics internal communication in the organisation. Then the attacker asks an employee to provide sensitive information for access to the computer network."*



*Evoluční teorie v podání spearphishingu.* [online]. [cit.15.2.2010]. Available from: <http://connect.zive.cz/content/evolucni-teorie-v-podani-spear-phishingu>

[22] Ibidem

[23] *Tip of the month July 2016 – Avoid getting hooked by Phishing.* [online]. [cit.14.8.2016]. Available from: <http://www.intermanager.org/cybersail/tip-of-the-month-july-2016-avoid-getting-hooked-by-phishing/>

[24] It is a combination of words "voice" and "phishing".

[25] It is a combination of words "SMS" and "phishing".

[26] E.g. **Xshqi** – *Android Worm on Chinese Valentine's day.* [online]. [cit.14.8.2016]. Available from: <https://securelist.com/blog/virus-watch/65459/android-worm-on-chinese-valentines-day/>

**Selfmite** – *Android SMS worm Selfmite returns, more aggressive than ever.* [online]. [cit.14.8.2016]. Available from: <http://www.pcworld.com/article/2824672/android-sms-worm-selfmite-returns-more-aggressive-than-ever.html>

## 4.7. Business Email Compromise (BEC)

Business Email Compromise[1] is a type of scam attack where an attacker impersonates an executive (typically the CEO), and attempts to get an employee, customer, or vendor to transfer money or sensitive information to the attacker.

The BEC scam could be linked to other forms of fraud like a romance, lottery, employment, and rental scams.

By the definition of FBI the BEC is *a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorised transfers of funds.*[2]

Unlike a traditional phishing attack, BEC is targeted at a certain individual or organisation. In the case of BEC, the attacker prepares for the attack very thoroughly and tries to obtain maximum information about the victim before the attack takes place. Usually they use websites, annual reports, information about the organisation's employees from social networks, from compromised email accounts, etc.

*This high level of targeting helps these email scams to slip through spam filters and evade email whitelisting campaigns. It can also make it much, much harder for employees to recognize the email is not legitimate.*[3]

The victims of the BEC scam range from small businesses to large corporations. The BEC scam is linked to other forms of fraud, including but not limited to: romance, lottery, employment, and rental scams.

The FBI warned that BEC scams would likely „continue to grow, evolve, and target businesses of all sizes.“ The FBI also mentioned that they've seen a 1,300% increase in business email compromise attacks since January 2015.[4]

The BEC attackers rely heavily on social engineering tactics to trick unsuspecting employees and executives. Some of the sample email messages have subjects containing words such as **request, payment, transfer**, and **urgent**, among others.

The BEC scam usually takes one of the following forms:

### 1. CEO Fraud

Attackers pose as the company CEO or other company executive and send a spoofed email to employees with the ability to send wire transfers, and instruct them to send funds to the attackers.

### 2. Fake Invoice[5]

A business, which often has a long standing relationship with a supplier, is requested to wire funds for invoice payment to an alternate, fraudulent account. The attacker typically approaches the victim via e-mail or telephone. An e-mail attack has typically a spoofed email source code (header) and subject of the request so it appears very similar to a legitimate request.

### 3. Account Compromise

This attack is similar to Fake Invoice. The attacker uses an employee's email account (hacked or spoofed), then sends an email to customers to announce them there has been a problem with their payment and they need to re-send it to a different account.

### 4. Business Executive and Attorney Impersonation

Victims are contacted by attackers, who identify themselves as lawyers or representatives of law firms. The attacker requests a large funds transfer to help settle a legal dispute or pay an overdue bill. The attacker is trying to convince victims that the transfer is confidential and time-sensitive, so it is less likely that the employee will attempt to confirm whether they should transfer the funds.

### 5. Data Theft

A type of BEC whose goal is not a direct money transfer. Typical victims of that attack include finance or HR departments /employees. The attacker requests them to send highly sensitive to his account. The social engineering is used and the data theft attack can be a starting point to the above mentioned BEC attacks focused on financial transfer.

Since 2017, there has been a dramatic increase in fraudulent attacks having the character of BEC in the Czech Republic. Yet again, most BEC attacks use similar modus operandi:

**1. Picking a victim and obtaining information about the victim** (medium-sized and small organizations are the most common target)

**2. Preparation of a spoofed email** (to create a spoofed email, publicly available free services are used very often, e.g.: [www.5ymail.com](http://www.5ymail.com). This service allows the attacker to create and send any spoofed email which corresponds to an existing email. However, this service does not make it possible to receive answers and therefore it is necessary to redirect the email communication to another existing email, registered e.g. with a freemail service. The real identity can be found from the message source code.)

**3. Sending a spoofed email to an employee of the victim** (the most frequent BEC attacks include CEO Fraud and Fake Invoice. Sums required in this way usually range from several hundred euros to € 4000.)

**4. Request for an immediate or "urgent" transfer of money to an account of the attacker or money mules** [validation of the payment, as well as of the person who gives the command to make the payment, is the key moment when the completion of the criminal act can be prevented. If the organization has appropriately set up security protocols, such transfer usually does not take place. From the point of view of identification of the

attacker, the attacker's account, or the account of money mules, is the tool which makes it possible to determine in practice whether it is the case of continuation of a criminal act (i.e. from the point of view of substantive criminal law one criminal act) or whether it is a case of concurrence of criminal acts. At the same time, it is de facto the most significant digital footprint which allows identification of the attacker.]

## 5. Money transfer to an account of the attacker or money mules

---

[1] BEC scams are also known as „CEO fraud“ or „Man-in-the-Email“ scams.

[2] *Business E-mail Compromise: The 3.1 Billion Dollar Scam*. [online]. [quote 12.6.2018]. Available at: <https://www.ic3.gov/media/2016/160614.aspx>

[3] *What is a Business Email Compromise (BEC) Attack? And How Can I Stop It?* [online]. [quote 12.6.2018]. Available at: <https://blog.barkly.com/what-is-a-business-email-compromise-bec-attack-and-how-can-i-stop-it>

[4] *Business E-mail Compromise: The 3.1 Billion Dollar Scam*. [online]. [quote 12.6.2018]. Available at: <https://www.ic3.gov/media/2016/160614.aspx>

[5] This attack is also called: "The Bogus Invoice Scheme," "The Supplier Swindle," and "Invoice Modification Scheme."

## 4.8. Fraudulent websites (companies)

On the Internet, you can find a number of activities, or websites, [1] presenting amazing prizes or offering various goods at very reasonable prices. Attackers use social engineering and rely primarily on people's trustworthiness and carelessness. The attacker's own activity can then typically take two forms.

In the first case, an attacker tries to lure sensitive data (e.g. name, surname, delivery address, e-mail, telephone number and password) typically for the purpose of registration, delivery of goods, prizes, etc. All these data are entered by a user and voluntarily. An attacker thus accesses data that he can, as in the case of phishing, use for a wide range of activities. For example, based on the password entered and other information about a user, an attacker may try to gain access to other services that a user uses. [2].

In the other, much more common case, these are activities that consist in fraudulently luring funds from a user. Cars, motorcycles, tractors, other agricultural machinery and, above all, electronics of any kind are usually offered on the Internet at a very advantageous price.

With regard to fraudulent offers on the Internet, the European Consumer Centre [3] has issued a recommendation for users, which should enable them to identify fraudulent practices:

- **Enter the company information (e.g. company name, website address, e-mail) in an Internet search engine.**
- **Think about how the merchant presents itself.** Does the website where you are going to buy something look professional? E-mail addresses on free and anonymous servers such as yahoo.com, hotmail.com, gmail.com, live.com, seznam.cz, etc. will certainly not create a credible impression. Likewise, if the website is located on a free hosting server, it is sign of unprofessionalism.
- **Pay only in advance if it is a truly trustworthy merchant.** You certainly won't give money on the street to a stranger with the promise that he/she will deliver the thing to you in the future. However, many users do this on the Internet. Only make a payment in advance if you are sure you are dealing with a trusted supplier. In particular, payment card details need to be protected.
- **A request for payment by Western Union is particularly suspicious.** For bank transfers, never send money to private accounts unless it is the account of the selling company.
- **The usual signs of fraud include poor language, the requirement to pay in advance in cash or by bank transfer, other requests for payments under a fictitious pretext (customs, insurance, packaging of a larger number of pieces of the product) and so on. Remember that if an offer seems too good to be true, it probably is not real!**
- **Check the country's business register to see if the company is registered.** (It also happens that someone misappropriates the name of an existing company and starts a website with a similar name.
- **Check the website domain.** It happens that a web address is the same as the address of a real and registered company. However, there is one difference – the domain, i.e. the suffix of the Internet address, is different (e.g. not ".co.uk" for Great Britain, but ".co.cc" for the Cocos Islands).
- **Find the company's headquarters on an internet server offering street photography of cities,** according to the address given in the advertisements and on the company's website.
- **Value your personal information.** Do not share information about yourself on untrusted or unknown sites. Only provide information that is really necessary.
- **Do not respond to spam.** Do not respond to unsolicited e-mails, in any case do not disclose your bank account details, payment card number or, for example, login details to internet banking by e-mail. Delete junk e-mail, never open unknown attachments. [4]

All of the above features are to be considered as mere indications that may lead to the detection of fraud. An attacker can modify his actions based on the success of his own attack. **In addition to these tips, it is advisable to use the warnings published on other sites, such as [www.podvodnefirmy.cz](http://www.podvodnefirmy.cz) etc.**

### Possibilities of criminal sanctions in the Czech Republic

In the Czech Republic, it is possible to punish the conduct described above under **Section 209** (Fraud) of the Criminal Code. The fraud is completed by enrichment. A creation of a replica of a website and the acquisition of login names and passwords could then be qualified as a preparation or attempt of a criminal offence according to Section 209 of the Criminal Code. If an attacker attempted (Section 21 of the Criminal Code) unauthorised access to another user's account using the obtained access data, such conduct could also qualify under **Section 230** (Unauthorised access to the computer system and information carrier) of the Criminal Code.

### Possibilities of criminal sanctions in Poland

In Poland this is regulated by Art. 286 (fraud), which says that:

§ 1. Whoever, in order to gain a material profit, leads another person to a disadvantageous disposal of his own or another person's property by means of deception or exploitation of an error or incapacity to grasp an intended action, shall be subject to the penalty of deprivation of liberty for a term of between 6 months and 8 years.

### Possibilities of criminal sanctions in Portugal

Again, as explained regarding phishing in general, such acts would be punishable as Computer-related forgery (Art. 3 of the Cybercrime Law), as well as Computer-related fraud (Art. 221 of the Criminal Code).

[1] The most common are websites, advertising portals, but it can also be accounts on social media, etc.

[2] Very often, the same or similar password is entered by users within different online services. As a result, an attacker can use, for example, the technique of dictionary attack to hack into access data to other services. By this action, the attacker may also commit other illegal actions (e.g. see chapter 4.15 [Identity theft](#), 4.8 [Hacking](#) etc.).

For more details, see e.g. *Slovníkový útok*. [online]. [cit.30.8.2016]. Available from: <https://managementmania.com/cs/slovnikovy-utok>

[3] For more details, see <http://www.evropskyspotrebiteľ.cz/>

[4] For more details: see *ESC radí, jak poznat podvody na internetu*. [online]. [cit.30.8.2016]. Available from: <http://www.evropskyspotrebiteľ.cz/nakupy-online/esc-radi-jak-poznat-podvod-na-internetu-27250>

## 4.9. Hacking

The term hacking is currently perceived by the public pejoratively as any activity of a person aimed at gaining illegal access to another's system or personal computer.<sup>[1]</sup> Especially in the media, this term is generally referred to as all attackers whose actions are directed against information technologies or whose activities are based on the use of such technologies. In this context, however, there is a fundamental difference between the public's perception of the content of the concept of hacking and those of themselves who call themselves hackers or are labelled as such by their own community.

The terms "hacker"<sup>[2]</sup> and "hacking" originated in the USA, in the 1950s, and referred to a **technically gifted person** (and his/her activities) **who was able to find new, often unorthodox, solutions to a problem.**

To understand how attackers, which we used to refer to as hackers, perceive society and its rules, it is useful to know their opinion. In 1984, Levy defined the following principles of hacking ethics:

1. Access to computers and anything else that can teach you something about how the world works should be unlimited and absolute. Always respect the rule of personal experience.
2. All information should be free of charge.
3. Do not trust the authorities, support decentralisation.
4. Hackers should be judged by their actions and not by misguided criteria such as age, race or status.
5. You can create "beauty" on a computer.
6. Computers can change your life for the better.<sup>[3]</sup>

Although these rules are not always respected or acknowledged, they represent the basic framework for the perception of the virtual world by attackers, whom we call hackers.

Another important insight into the perception of the world through the eyes of a hacker is the document *The Hacker Manifesto*:

*The following was written shortly after my arrest...*

### ***The Conscience of a Hacker***

*Another one got caught today, it's all over the papers. "Teenager Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"...*

*Damn kids. They're all alike.*

*But did you, in your three-piece psychology and 1950's technobrain, ever take a look behind the eyes of the hacker? Did you ever wonder what made him tick, what forces shaped him, what may have molded him?*

*I am a hacker, enter my world...*

*Mine is a world that begins with school... I'm smarter than most of the other kids, this crap they teach us bores me...*

*Damn underachiever. They're all alike.*

*I'm in junior high or high school. I've listened to teachers explain for the fifteenth time how to reduce a fraction. I understand it. "No, Ms. Smith, I didn't show my work. I did it in my head..."*

*Damn kid. Probably copied it. They're all alike.*

*I made a discovery today. I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up. Not because it doesn't like me...*

*Or feels threatened by me...*

*Or thinks I'm a smart ass...*

*Or doesn't like teaching and shouldn't be here...*

*Damn kid. All he does is play games. They're all alike.*

*And then it happened... a door opened to a world... rushing through the phone line like heroin through an addict's veins, an electronic pulse is sent out, a refuge from the day-to-day incompetencies is sought... a board is found.*

*"This is it... this is where I belong..."*

*I know everyone here... even if I've never met them, never talked to them, may never hear from them again... I know you all...*

*Damn kids. Tying up the phone line again. They're all alike.*

*You bet your ass we're all alike!*

we've been spoon-fed baby food at school when we hungered for steak... the bits of meat that you did let slip through were pre-chewed and tasteless. We've been dominated by sadists, or ignored by the apathetic. The few that had something to teach found us willing pupils, but those few are like drops of water in the desert.

***"This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.***

***Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for. I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.***

Mentor

Hacker's Manifesto

8 January 1986

Currently, hackers themselves use the term hacker for people who have excellent knowledge of information and communication systems, computer systems, their operating systems and other programs, their networking principles and mechanisms, and are also excellent programmers capable of creating their own software, namely in a very short time. It is the effort to know how information technology, applications or technical means work, and to make this information available to other users, what is the driving force and philosophy of many people. The ability of a hacker to gain access to computer systems through his/her own designed and written computer programs even outside the usual methods of access (which does not necessarily mean that gaining such access must be motivated by trying to cause harm, other harm or otherwise get rich) is one, not the only skill.

### **Division of hackers**

It is the motivation to obtain atypical (not necessarily illegal) access, the method of performing such an intrusion, their motivation and possible handling of the obtained data, what are the key factors for distinguishing these persons into the following three basic groups:

**White hats** – these are hackers who infiltrate a system using security vulnerabilities of the system precisely in order to detect these gaps in security and create such mechanisms and barriers that should prevent such attacks. They are often employees or external collaborators of renowned companies doing business in the field of information technology. Their intrusion into a system does not cause damage or other harm to users, on the contrary, in many cases they alert the administrator of such an infected system to security flaws. Their activity is fundamentally non-destructive in nature.

**Black hats** – basically the opposite of the white hat hackers. Their motivation is an attempt to cause damage or other harm to a user of an infected system, or to obtain property or other benefit. In addition to the actual achieved breach of a hacked system, another, criminal element is evident in their actions.

**Grey hats** – this is a grey zone of hackers, i.e. people who have not profiled towards the two groups. Occasionally, they may violate some rights of others or moral principles, but their activities are not primarily driven by the desire to cause harm, as is the case with black hats.

In addition to the above, i.e. the most commonly used division, it is possible to divide hackers into other groups based on their motives. These are: Script kiddies, hactivists, state-sponsored hackers, spy hackers, cyber terrorists, beginners (n00b), blue hat hackers, etc..[\[4\]](#)

A key factor in assessing hacking as a potential security threat is to determine the reason for the hacker's activities (see the division of hackers). In some cases, hacking can pose a real security threat, as it is a breach of computer system security, or a breach of protection or exploitation of system vulnerabilities. On the contrary, in other cases, it may be a suitable complement to increase the security of a system as a whole or to find weak spots and vulnerabilities.

In general, hacking can be really described as any unauthorised intrusion into a computer system from the outside, most often within the Internet. However, not every hacker attack is necessarily a crime.

The danger of hacking activities lies, among other things, in the fact that in addition to gaining unauthorised access to an attacked system (regardless of the hacker's motivation), these people create and use highly effective software tools, the source code of which is often subsequently published by hackers themselves, e.g. within the darknet markets. This can lead to further mass abuse of these programs by users who do not have the control to create such programs themselves, but due to the existence of tools made available in this way, they can potentially cause relatively significant damage to users of infected systems. Through the Internet, it is thus possible to obtain often complete sets of hacker software programs containing basic software and information necessary for its use, practically without in-depth knowledge of the operation of these programs.

### **Forms of hacking**

The actual activity of hackers comprises a number of actions. Typical activities used by hackers include:

1. Social engineering
2. Password cracking.[\[5\]](#)
3. Port scanning.[\[6\]](#)
4. Using malware to infiltrate a computer system
5. Phishing
6. Cross Site Scripting.[\[7\]](#)

7. Eavesdropping on communication.[8]

### Well-known hacker groups and hackers

Probably the best known current hacker group is Anonymous, but there are or were other groups:[9]



- Anonymous
- Lizard Squad
- The Level Seven Screw
- Chaos Computer Club
- Lulzsec
- Syrian Electronic Army
- Globalhell
- Network Crack Program Hacker Group
- Antisec Movement
- Legion of Doom (1984-2000)
- Masters of Deception (1989-1993)
- Milw0rm etc.

The **best-known hackers** include Jonathan James, Vladimir Levin, Gary McKinnon, John McAfee, Astra, Stephen Wozniak, James Kosta, Kevin Mitnick, Adrian Lamo, David L. Smith.[10]

There is no doubt that **not all hacker activity is legal**. In relation to interference with the computer system, guaranteed fundamental human rights and freedoms will certainly be violated.

### Possibilities of criminal sanctions in the Czech Republic

As mentioned above, there are a number of actions or attacks that can be classified as hacking (starting with password cracking and ending with a complicated phishing attack that is combined with social engineering and the use of malware).

Actions of a hacker, consisting only in the use of his abilities, due to which he overcomes security measures and gains access to a computer system or its part, can be punished according to **Section 230(1)** (Unauthorised access to computer system and information carrier) of the Criminal Code.

In the case of combined forms of attacks, where, for example, malware is used to infect a computer, such action of an offender must also be punished under **Section 230 (2)** (Unauthorised access to the computer system and information carrier) of the Criminal Code. If the aim of an attack is to gain an unjustified benefit to oneself or to another, or to unjustifiably limit the functionality of a computer system or other technical device for data processing, it is also possible to apply the provisions of **Section 230 (3)** of the Criminal Code.

### Possibilities of criminal sanctions in Poland

The offence of hacking is regulated in Art. 267§1 of the Penal Code.

*Whoever without authorisation gains access to information not intended for him, by opening a closed letter, connecting to the telecommunications network or breaking or bypassing electronic, magnetic, IT or other special security thereof, shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to 2 years.*

Breaching electronic security is one of the statutory elements of a crime under Article 267 (1) of the Criminal Code. "Securing an account with a password (code) is an obstacle in gaining access to information by an unauthorised person. Overcoming this obstacle by using an access code by the perpetrator against the will of the authorised person should be treated as a breach of electronic security. The use of such a code (password) by an unauthorised person against the will of the account owner breaks the electronic obstacle protecting access to either a bank account or a user account on an internet portal" (judgment of the District Court in Świdnica of 10 April 2019, reference number: IV Ka 112/19). The hallmarks of this crime include, in addition to „breaking or bypassing electronic, magnetic, IT security, consisting in the removal of special structures, covers, which are used to prevent access to information stored in the system“ the provision also covers the breaking of specific information safeguards other than electronic, magnetic or IT, which means that it is about such safeguards, the removal of which requires the perpetrator to have specialised knowledge or have specialised tools. In any case, breaking the security should cause some difficulties – then it can be assumed that such security is of "special" nature. Breaking the security might be a direct interference with the security system, usually destroying it, or bypassing the security without making any interference in it. For the implementation of the features of Art. 267 §1, it is necessary to break such a security, the main function of which is to protect information against unauthorised access to it. According to the judgment of the District Court in Świdnica of April 10, 2019, reference number: IV Ka 112/19, "the essence of the offence under Art. 267 §1 of the Penal Code is that the perpetrator does not know the security method (e.g. access codes to specific information or the content of passwords) after applying, taking certain actions (including e.g. deciphering the code or password to access information) or breaks such a special security or special security is avoided. It is not a crime under Art. 267 §1 of the Penal Code "obtaining information for which no protective measures have been taken, unless it consists in connecting to a telecommunications network".



Summarising the above considerations, it follows that according to the judgment of the Administrative Court in Szczecin of October 14, 2008, reference number: II AKa 120/08, "a person does not commit a crime under Art. 267 §1 of the Penal Code if they gained unauthorised access to information without breaking or bypassing a security feature, even if they do so by trickery". According to the judgment of the District Court in Świdnica of April 10, 2019, reference number: IV Ka 112/19, it follows from the above that "gaining access, without authorisation, to the information referred to in art. 267 §1 of the Penal Code by e.g. using a password provided or previously shared by the aggrieved party, or e.g. a password remembered by a web browser, or leaving the computer with the password for a given account entered and after that logging into the system it cannot be considered a password breach, so the above does not constitute an offence under Art. 267 §1 of the Penal Code". The hacking offence is prosecuted at the request of the aggrieved party.

### Possibilities of criminal sanctions in Portugal

In itself, the illegal access to a computer system is punished (Art. 6(1) of the Cybercrime Law). Moreover, the overcoming of security measures and / or the gain of a non justified gain are not required as objective elements, being considered as aggravated offences (Art.6(3) and (4).

As stated previously, the illegal creation, distribution or dissemination of any computer programme, executable instruction, code or data intended to perform an illegal access to a computer system is penalised as being an illegal access (Art. 6(2) of the Cybercrime Law.

---

[1] For more details cf. e.g. GRIFFITHS, Mark. Computer Crime and Hacking: a Serious Issue for the Police? *The Police Journal*, 2000, vol. 73, No. 1, pp. 18–24.

YAR, Majid. Computer Hacking: Just Another Case of Juvenile Delinquency? *The Howard Journal*, 2005, vol. 44, No. 4, pp. 387–399.

[2] This term can be translated in many ways and needs to be based on context. In American jargon, this originally meant riding aimlessly on horseback. A "hack" also referred to a simple solution to a problem. Subsequently, it meant committing some wrongdoing by university students.

[3] LEVY, Steven. *Hackers: Heroes of the Computer Revolution* Sebastopol, CA: O'Reilly Media, pp. 32–41. ISBN 978-1449388393.

Also available online:

<https://e11c1b148f6c7c56754c9184e0d1c52ac4d888f9-www.googleusercontent.com/host/OByAMXZl2-PZOWjBPYmhaWVVRN0E>

[4] For more details, see e.g.: SHNEIER, Bruce. *The Seven Types of Hackers*. [online]. [cit.16.8.2015]. Available from: [https://www.schneier.com/blog/archives/2011/02/the\\_seven\\_types.html](https://www.schneier.com/blog/archives/2011/02/the_seven_types.html)

*7 Types of Hacker Motivations*. [online]. [cit.16.8.2015]. Available from: <https://blogs.mcafee.com/consumer/family-safety/7-types-of-hacker-motivations/>

*7 Types of Hackers You Should Know*. [online]. [cit.16.8.2015]. Available from: <https://www.cybrary.it/Qp3n/types-of-hackers/>

[5] It is the process of obtaining a password to a computer system. The following are commonly used to crack passwords:

- Guessing a password by brute force (testing a password. A strong enough password is a prevention);
- Guessing a password based on certain knowledge about a user (obtained for example on social networks, etc.);
- Use of a dictionary of commonly used passwords (dictionary attack);
- Requesting the password from the system administrator by impersonating an authorised user (An attacker impersonates a forgotten password and attempts to recover it.)
- Capturing passwords from unencrypted or insufficiently encrypted network communication between the computer system and a user
- Searching for passwords in data files stored by a system

[6] This is a method that detects open network ports on a computer system that is connected to a computer network. Based on this finding, it is possible to determine which services are running on the computer system (e.g. web server, ftp server, etc.). The actual attack is then focused on the detected running services based on their vulnerabilities.

[7] This is a website intrusion attack. This type of attack uses active elements (scripts) on the website, in which malicious code is inserted and then offered to the victim.

One of the less common, but all the more dangerous, actions is to exploit a web application vulnerability to run malware within a victim's browser. The victim is then unable to detect such behaviour. The malicious code runs the same as the rest of the page, and the attacker is allowed to take over the browser permissions within the system.

For more details, see e.g. OWASP, XSS [online]. [cit.15.7.2016]. Available from: [https://www.owasp.org/index.php/Cross-site\\_Scripting\\_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)).

[8] See chapter 4.12 *Sniffing*.

[9] For more details, see e.g. *10 Most Notorious Hacking Groups*. [online]. [cit.15.7.2016]. Available from: <https://www.hackread.com/10-most-notorious-hacking-groups/>

Figure taken from [online]. [cit. 15.7.2016]. Available from:

[http://img02.deviantart.net/a2fd/i/2012/330/7/5/we\\_are\\_anonymous\\_by\\_mrj\\_5412-d5mb6xc.jpg](http://img02.deviantart.net/a2fd/i/2012/330/7/5/we_are_anonymous_by_mrj_5412-d5mb6xc.jpg)

[10] For more details, see e.g. *10 Most notorious hackers of all time*. [online]. [cit.15.7.2016]. Available from: <https://hacked.com/hackers/>

*Nejznámější počítačové hackeři a jejich útoky.* [online]. [cit.15.7.2016]. Available from: <https://www.stream.cz/top-5/10004402-nejznamejsi-pocitacovi-hackeri-a-jejich-utoky>

## 4.10. Cracking

The term **cracking** is associated with the term hacking, sometimes even these terms are incorrectly confused by the public or in the media. The term can be translated into Czech as "louskání" or "pukání". In terms of content, the term cracking means breaking or circumventing the protective elements of a computer system, programs or applications, with the intention of their subsequent unauthorised use.

Crackers are often hackers from the black hat category, i.e. those who make breakthroughs in systems in an attempt to cause damage to a user, obtain information, or enrich themselves or others. Furthermore, cracking is mainly associated with copyright and related rights infringement. In this sense, cracking is an act consisting in the circumvention of protective elements that prevent the creation of copies or the illegal use of computer programs and music or film products (film or music CDs, DVDs, etc.). These security elements are used as means of copyright protection in the sense of Section 43 (1) of the Copyright Act, as amended.

One of the forms of cracking is "**password cracking**" used to determine the access password to a computer system, licensed system or program. When it comes to copyright infringement, a cracker usually creates a keygen or crack<sup>[1]</sup>, which allows the subsequent use of the program. Programs modified in this way are usually shared on warez forums or P2P networks.

### Possibilities of criminal sanctions in the Czech Republic

Actions of an offender, within which the protection of a computer system or program is breached, with the intention of obtaining information and their subsequent unauthorised use, fulfills the objective elements of a criminal offence under **Section 230 (1) or (2)** (Unauthorised access to computer system and information carrier) of the Criminal Code. If the aim of a cracking attack is to gain an unjustified benefit for oneself or another, it is also possible to apply the provisions of **Section 230 (3)** of the Criminal Code.

Criminal liability under **Section 231** (Measures and storage of the access device and password to the computer system and other such data) of the Criminal Code is not excluded either. During the distribution of a protected copyright work, **Section 270** (Infringement of copyright, rights related to copyright and rights to the database) of the Criminal Code is fulfilled.

### Possibilities of criminal sanctions in Poland

The same laws apply as for hacking.

### Possibilities of criminal sanctions in Portugal

As mentioned, the illegal creation, distribution or dissemination of any computer programme, executable instruction, code or data intended to perform an illegal access to a computer system is penalised as being an Illegal access (Art. 6(2) of the Cybercrime Law), as aggravated offence if the offender had access to a trade secret or confidential data, the same in case of a relevant unjustified benefit (Art. 6(4) of the Cybercrime Law).

Again, the circumvention of any effective technological measures related to rights-management information is criminalised (Arts. 217 to 219 and 224-224 of the Code of Copyright and Related Rights).

---

[1] **Keygen** – Key Generator. Program generating serial numbers or other data. **Crack** – a program used to remove or reduce the functionality of protection elements of another program.

## 4.11. Internet (computer) piracy

*Each author has the right to determine how his/her work will be handled.*

*If I do not agree with the terms of use of the work,*

*understand them or know them,*

*I have the right not to use the work.*

Jan Kolouch

The term Internet piracy is a general term that covers crime, which infringes intellectual property rights (very often limited to copyright). Only with the expansion of computer systems and especially the advent of the Internet can we talk about mass piracy as one of the most widespread forms of cybercrime.

Infringement of intellectual property rights, in particular copyright and related rights, is currently one of the most pressing issues in the information technology environment.

### 4.11.1. Intellectual property law

In relation to internet piracy, it is first necessary to define the issue of intellectual property, especially copyright. This definition is necessary to understand the difference between the legal and illegal actions of those who are active on the Internet.

An intellectual property right is an intangible asset, so-called "intangible property", which is the **result of a person's creative activity**. This right is **independent of the material substrate** (it can therefore be used anytime and anywhere in the world) provided that it is **unique, unrepeatable and sufficiently original**.

Intellectual property rights can be divided into two areas:

1) **Copyrights** (protect, for example, original literary and artistic works, musical compositions, television broadcasts, computer programs, databases, advertising creations, multimedia, etc.)

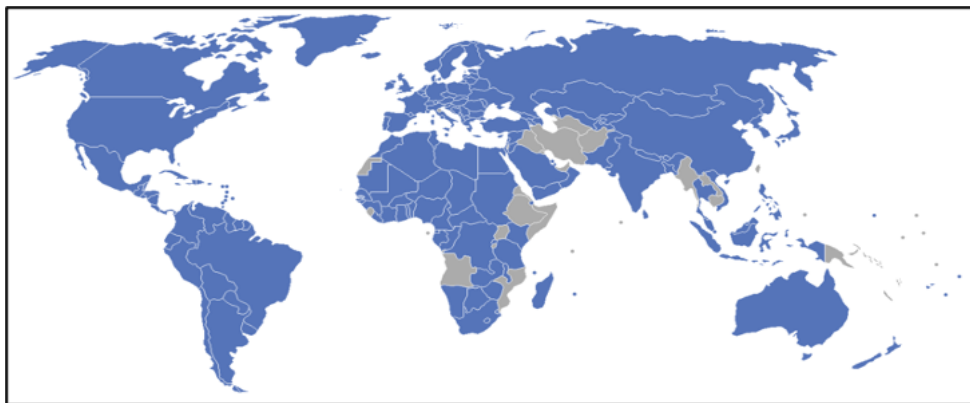
2) **Industrial rights** (protect, for example, patents for inventions, designs, industrial models, trademarks, geographical origin, etc.)

In terms of the focus of this monograph, I will primarily deal only with copyright and interference with this right.

### 4.11.2. Legislative framework

Copyright protection first began to be addressed at the international level in the 19th century, and the most important legal documents dealing with it include:

· Berne Convention for the Protection of Literary and Artistic Works [\[1\]](#) (1886), which was subsequently supplemented and amended [1908 (Berlin), 1928 (Rome), 1948 (Brussels), 1967 (Stockholm), 1971 (Paris)]. Since 1967, it has been managed by WIPO (World Intellectual Property Organization).



**List of states. States which have adopted the Berne Convention are marked in blue.** [\[2\]](#)

· Agreement on Trade-Related Aspects of Intellectual Property Rights, which is one of the annexes to the Agreement establishing the World Trade Organization (WTO) – see Notification No. 191/1995 Sb., (**TRIPS – Trade Related Aspects of Intellectual Property Rights**)

· International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations of 26<sup>th</sup> October 1961 (Decree No. 192/1964 Sb., as amended by Corrigendum No. 157/1965 Sb.) – **Rome Convention**

World Intellectual Property Organization Copyright Treaty Geneva 1996 of 20 December 1996 (see Not. No. 33/2002 Sb. of Int. Treaties), (**WCT – WIPO Copyright Treaty**)

- World Intellectual Property Organization Performances and Phonograms Treaty Geneva 1996 of 20 December 1996 (see Not. No. 48/2002 Sb. of Int. Treaties), (**WPPT – WIPO Performances and Phonograms Treaty**)
- Convention for the Protection of Producers of Phonograms against Unauthorized Reproduction of their Phonograms of 29 October 1971 (see Decree 32/1985 Sb.) – **Geneva Convention**
- General Copyright Convention revised at Paris on 24 July 1971 (see Decree No. 134/1980 Sb.)
- Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs,
- Council Directive 92/100/EEC of 19 November 1992 on rental right and lending right and on certain rights related to copyright in the field of intellectual property, as amended,
- Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission,
- Council Directive 93/98/EEC of 29 October 1993 harmonizing the term of protection of copyright and certain related rights, as amended,
- Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases,
- Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society,
- Directive 2001/84/EC of the European Parliament and of the Council of 27 September 2001 on the resale right for the benefit of the author of an original work of art,
- Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights.
- Council of Europe Convention No. 185 on Cybercrime.

### 4.11.3. Attacks

Several terms have been used in the Internet environment for the phenomenon of copyright and related rights infringement. The terms **software piracy** (for copyright infringement in relation to computer programs) and **audiovisual piracy** (for copyright infringement of audiovisual works – music and film) are most often used. **However, the basis for software and audiovisual piracy is always an infringement of one of the copyrights or rights related to copyright.** A general term that covers software and audiovisual piracy is Internet (sometimes also computer) piracy.

Crimes against intellectual property have expanded considerably with the mass advent of the Internet. The most common cases of copyright infringement in cyberspace are:

- *dissemination of a work by e-mail*, which is the easiest way to distribute small files (especially literary or graphic copyright works),
- *publication of a work on a website* without the author's consent. This is another very simple way of infringing copyright. Smaller files are published (in terms of data size) and this illegal behaviour is usually detected very early.
- *dissemination of a work by uploading to a specialised server*, from where it is possible to download the works freely (e.g. Megaupload, Rapidshare),
- *dissemination of a work using Peer-to-Peer (P2P) networks*.<sup>[3]</sup> These networks are capable of transmitting/sharing huge amounts of data (in the order of several GB to tens of TB). They are the most egregious cases of copyright infringement.
- *interference with computer programs in order to overcome the technical measures of the copyright holder preventing the making of copies of such protected programs* (so-called crack),
- *dissemination of a work using data carriers directly between users* (lending and subsequent copying of data from DVD, HDD, etc., sale of data carriers and others),
- *recording directly during a projection and subsequent dissemination of the recording* (e.g. recording a film work directly from the screen) – camcording,
- *unauthorised screenings of audiovisual works*,
- *an actual acquisition of a computer work*. A computer program is specially protected and it is not possible to make copies of such work, even for personal use, without the consent of the copyright holders within the meaning of copyright law,
- *use of a computer program in violation of the licence*,
- and more.

The most common forms of audiovisual piracy include, in particular, unauthorised distribution of audiovisual works via computer networks, recording of cinematographic works directly in cinemas and their subsequent "posting" for download in cyberspace, distribution of original media with a film or music in violation of a licence agreement, production and the dissemination of counterfeits of original cinematographic or musical works and the public screening of cinematographic works in breach of a licensing agreement. Furthermore, conduct consisting in the dissemination of software products, interventions in software products, illegal production of software products and the use of software products in violation of the license agreement. Copyright infringement will already be an unauthorised acquisition of a software product without further treatment.

**Placing a work** (regardless of whether it is audiovisual or software) in cyberspace (**upload**) means dissemination of the work in the sense of copyright law and (unless allowed by the author or another authorised person) may be punishable. **Unauthorised use of a work is also a publication of a link to a place in cyberspace from where a work can be obtained.**

For comparison with foreign legislation, it is suitable to mention the French HADOPI law,<sup>[4]</sup> which was supposed to protect against internet piracy. According to this law, a special office was established tasked with detecting illegal downloads of copyrighted material. Those users who downloaded music and movies from the Internet free of charge (excluding freely distributable works) were warned three times, and if these warnings were not heeded, the authority was entitled to disconnect them from the Internet for up to one year.<sup>[5]</sup> However, even such a strict law did not limit the number of illegal downloads of copyrighted works. At the same time, however, it raised a number of questions concerning the admissibility of interference with fundamental human rights and freedoms without a court decision.<sup>[6]</sup> The HADOPI law was repealed on 10 July 2013.

The term "Warez" often appears in connection with Internet piracy. **Warez is**, very simply put, a **form of computer piracy**, where information technology is only a means of speeding up the distribution of illegal copies of copyright works over the Internet. Warez forums are currently used mainly to download cracks and keygens, as well as complete modified programs, movies and music. The final product of the warez scene is called **release**. To protect privacy, clients of warez forums use proxy servers and bouncers to mask their IP address, thus preventing possible monitoring. The actual communication and release offering takes place in private rooms created for this purpose on the Internet, to which only members of the group have access.

### Possibilities of criminal sanctions in the Czech Republic

The provision of files, whether within warez or P2P networks, can be punished under **Section 270** (Infringement of copyright, rights related to copyright and database rights), or according to **Section 231** (Measures and storage of access devices and passwords to the computer system and other such data) of the Criminal Code.

### Possibilities of criminal sanctions in Poland

Intellectual property issues in Poland have been regulated by two basic legal acts: the Act on Copyright and Related Rights and the Industrial Property Law Act.

The Penal Code has two Articles about breaching or stealing intellectual property:

Article 115. 1. Whoever appropriates the authorship or misleads as to the authorship of the whole or a part of another person's work or artistic performance, shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to 3 years.

And Article 278 (theft)

§ 1 Whoever takes another's movable property for the purpose of appropriation shall be subject to the penalty of deprivation of liberty for a term of between 3 months and 5 years. § 2 The same punishment shall be imposed on anyone who, without the authorized person's consent, obtains another's computer program for the purpose of gaining a material profit.

### Possibilities of criminal sanctions in Portugal

In general, such acts are criminalised as unauthorised copying, distribution and selling of works and / or as Counterfeiting of copyrighted works (Arts. 195 and 196 of the Code of Copyright and Related Rights).

On the other hand, the Illegal reproduction of protected computer programme (Art. 8 of Cybercrime Law) and the Illegal reproduction or communication of a copyright protected database (Art. 11 of Decree-Law No. 122/2000) would apply, being the case.

---

[1] Available online. [online]. [cit.15.7.2016]. Available from: <http://portal.gov.cz/app/zakony/zakonPar.jsp?page=0&idBiblio=34669&nr=133-2F1980&rpp=100#local-content>; <http://www.zakonyprolidi.cz/cs/1985-19>

[2] *Bernská úmluva o ochraně literárních a uměleckých děl*. [online]. [cit.15.7.2016]. Available from: [https://cs.wikipedia.org/wiki/Bernsk%C3%A1\\_%C3%BAm%20mluva\\_o\\_ochran%C4%9B\\_liter%C3%A1rn%C3%ADch\\_a\\_um%C4%9Bleck%C3%BDch\\_d%C4%9B](https://cs.wikipedia.org/wiki/Bernsk%C3%A1_%C3%BAm%20mluva_o_ochran%C4%9B_liter%C3%A1rn%C3%ADch_a_um%C4%9Bleck%C3%BDch_d%C4%9B). The presented map is only illustrative and does not show the current geopolitical division of the world. A complete list of states that have ratified the WIPO Treaty can be found at: [http://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty\\_id=15](http://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty_id=15)

[3] By connecting to P2P, a user, by default, starts automatically sharing its content with other users (usually unknown to him). Typically, when downloading, the upload of the downloaded material is automatically set.

[4] **HADOPI** (High Authority for Copyright Protection and Dissemination of Works on the Internet law), Fr: *Loi favorisant la diffusion et la protection de la création sur Internet*.

[5] The Office did not need a court ruling for this decision. Based on the opinion of the Constitutional Court Fr. of 22 November 2009, court approval is required for disconnection.

[6] For more details, see e.g. *Francie zakáže internetové pirátství*. [online]. [cit.15.7.2016]. Available from: <http://www.blisty.cz/2009/5/13/art46807.html>

*Přísný zákon proti hudebním a filmovým pirátům Francii nepomohl.* [online]. [cit.15.7.2016]. Available from: [http://technet.idnes.cz/prisny-zakon-proti-hudebnim-a-filmovym-piratum-francii-nepomohl-phi-/sw\\_internet.asp?c=A100330\\_095705\\_sw\\_internet\\_vse](http://technet.idnes.cz/prisny-zakon-proti-hudebnim-a-filmovym-piratum-francii-nepomohl-phi-/sw_internet.asp?c=A100330_095705_sw_internet_vse)

*France drops controversial 'Hadopi law' after spending millions.* [online]. [cit.15.7.2016]. Available from: <https://www.theguardian.com/technology/2013/jul/09/france-hadopi-law-anti-piracy> etc.

## 4.12. Sniffing

Sniffing is a method of illegal interception of data passing through a computer network during communication between a provided service and a computer system via a **sniffer**.<sup>[1]</sup>

Technically, sniffing means capturing and reading TCP packets. From a security point of view, sniffing can also be described as network monitoring or network operation monitoring, and it is one of the standard tools for network diagnostics, or diagnostics of anomalies in network operation. Network monitoring is then able to display, for example, non-standard communication of a computer system infected with malware, etc. The network administrators' own activity in the case of network monitoring is not illegal (unless they commit further actions that could establish possible legal liability – such as installing a keylogger or other malware on a computer system without the user's knowledge), as it allows maintaining and managing a computer network.

A number of tools are used to monitor network traffic (e.g. Wireshark,<sup>[2]</sup> NetWorx, PRTG Network monitor, etc.).

For sniffing to fall under one of the categories of cybercrime, it is necessary for a person performing this activity to act illegally, typically without the consent or knowledge of a user. Using data captured by sniffing, an attacker is able to extract and compose sensitive information about a user, such as login data (username and password), e-mail or VOIP communication, information about used services, etc. Malware in the form of Trojans, keyloggers or spyware can also be used for sniffing.



Password Sniffer Spy. Names and passwords are blurred.<sup>[3]</sup>

### Possibilities of criminal sanctions in the Czech Republic

Such activity could practically be described as **illegal interception and recording of telecommunications traffic**. The conduct described above will certainly interfere with fundamental human rights and freedoms, in particular **Article 13** of the **Charter**, and it is **completely indifferent whether illegal sniffing is carried out by an external attacker or by a network administrator**. According to the norms of criminal law, it would be possible to subsume such conduct under **Section 182(1)** (Violation of the secrecy of transported messages) of the Criminal Code, and in case of misuse of information obtained in this way, it could be a criminal offence under **Section 182 (2)** of the Criminal Code. If the said illegal activity is performed by an employee of the operator of postal services, telecommunication services or computer system or anyone else performing communication activities, it could satisfy the objective elements according to **Section 185 (5)** of the Criminal Code.

### Possibilities of criminal sanctions in Poland

In Poland sniffing is an offence punishable according to:

Breach of secrecy of communication (sniffing) - Article 267 § 3 of the Penal Code.

### Possibilities of criminal sanctions in Portugal

Such acts are placed within the scope of Illegal interception (Art. 7 of Cybercrime Law), but also the access to and the sharing of any contents might be considered a Breach of correspondence or telecommunications (Art. 194 of the Criminal Code).



---

[1] **Sniffing** is an English word meaning snooping or spying around. A sniffer is then someone who sniffs, snoops or spies around.

[2] More details to use of Wireshark, see e.g. *How to use Wireshark to capture, Filter and inspect Packets*. [online]. [cit.15.7.2016]. Available from: <http://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/>

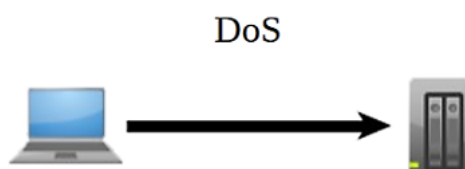
[3] *Password Sniffer Spy*. [online]. [cit.18.8.2016]. Available from: <http://securityxploded.com/password-sniffer-spy.php>

## 4.13. DoS, DDoS, DRDoS attacks

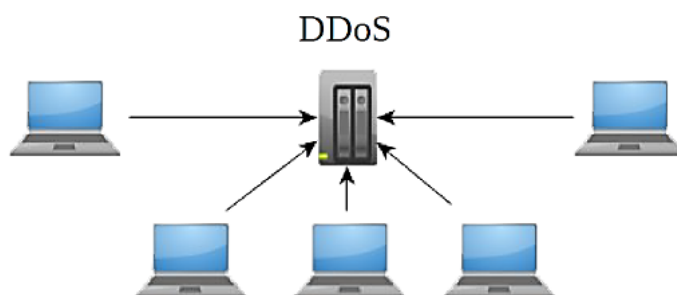
The term DoS is an abbreviation of "**denial of service**". This is one of the forms of attacks on an (Internet) service, the aim of which is to deactivate or reduce the performance of the infected technical equipment. [1] This attack is carried out by flooding a compromised computer system (or network element) with repeated requests for actions to be taken by the computer system. This attack can also be implemented by flooding information channels between the server and the user's computer or by flooding free system resources. A system mainly exhibits infection from a DoS attack through unusual slowdown of service, general or momentary unavailability of service (e.g. websites), etc.

The difference between DoS, DDoS and DRDoS attacks lies mainly in the way the attack is conducted. For clarity, figures demonstrating the method of the attack are attached to the individual types of attack.

In the case of **DoS (Denial of Service)**, the source of the attack is one. This type of attack is relatively easy to defend, as it is possible to block traffic from the source of the attack.

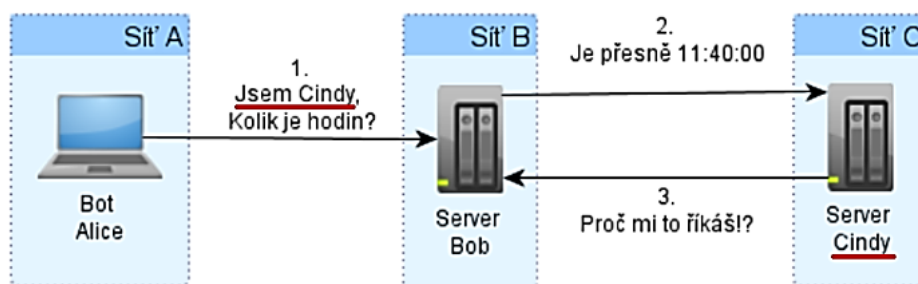


With **Distributed Denial of Service (DDoS)**, the target computer system is congested by **sending packets from multiple computer systems in various locations, making it difficult to defend against and identify the attacker**. Such attacks have been used, for example, against Yahoo! Inc., e-commerce, etc. [2] Botnets or activities of users supporting a certain online campaign are very often used for this type of attacks (see below – Anonymous and LOIC).



In the case of **DRDoS (Distributed Reflected Denial of Service)**, it is a spoofed distributed DoS attack that uses a so-called reflection mechanism. The attack consists of sending fake connection requests to a large number of computer systems, which then respond to these requests, but not to the initiator of the connection but to the victim. This is because spoofed connection requests have the victim's address as the source address, which is then flooded with responses to those requests. Many computer systems thus become an involuntary participant in an attack, in fact, by responding correctly to a connection request.

DoS, DDoS, DRDoS attacks very often use bugs such as the operating system, running programs or network protocols – UDP, TCP, IP, http, etc.



Text on the figure:

Network A, Bot Alice

1. I'm Cindy, What time is it?

Network B, Server Bob

2. It's exactly 11:40:00

Network C, Server Cindy

3. Why are you telling me this!?

There are several basic methods of DoS or DDoS attack, the most well-known ones are the following:

### - Flooding with ping command (Ping-Flood)

Due to the Internet Control Message Protocol and the Ping tool (Packet Internet Groper), it is possible to use the "ping" command to determine the "life" of a computer system with a given IP address and to detect the response time of such a system. As part of the Ping-Flood attack, a victim is flooded with a large number of so-called ICMP echo request packets, to which the victim begins to respond – sending so-called ICMP Echo Reply packets. An attacker hopes that this will overwhelm the victim's bandwidth (for receiving and sending data). The actual attack can be further intensified by setting the ping emitting ICMP packets option flood. The packets are then sent without waiting for a response. If the target computer system is underperforming, it can be made inaccessible.

### - Flooding of free system resources (SYN-Flood)

SYN-Flood is a type of attack in which an attacker tries to overwhelm his victim with a large number of connection requests. An attacker sends a sequence of packets with a SYN command (SYN packets) to the target computer system (victim), with the target system responding to each SYN packet by sending a SYN-ACK packet, but the attacker no longer responds. The target computer system waits for the final acknowledgment, the so-called ACK packet from the connection initiator (attacker) and holds the allocated resources for this connection, but it has a limited number. This can deplete the system resources of the target of the attack. [3]

### - Source address spoofing (IP spoofing)

IP Spoofing is an activity consisting in forgery of a source address of sent packets, when an attacker initiating a connection from machine A with the IP address **a.b.c.d** inserts e.g. IP address **d.c.b.a** as a source address and sends them to a target B. Target B then responds to this source address, i.e. the response is not addressed to the IP address a.b.c.d, but to the IP address **d.c.b.a**. Using this method, it is possible to make attacks worse (intensify attacks) such as DoS, DDoS. An attacker uses this technique when he does not need a response from his target to his connection request, he just wants to employ him. When an attacker specifies the IP address of the target of his attack (e.g. a.a.a.a) as the source IP address in the sent packets and sends the packets to many other computer systems (IP addresses), these then respond to the computer system a.a.a.a. In this way, a DRDoS attack is carried out.

### - Smurf attack

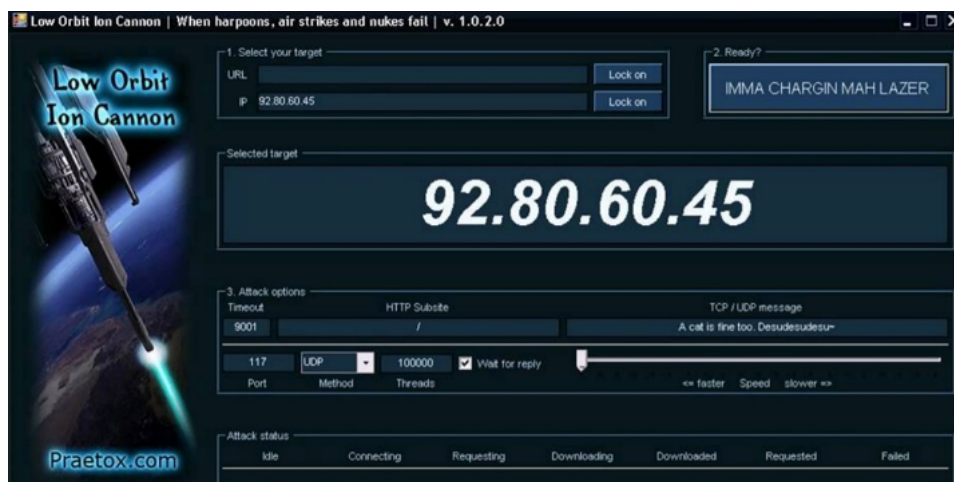
This attack is executed through a misconfiguration of the system, which allows the transmission of packets to all computers connected to the computer network through the broadcast address.

The goal of DoS/DDoS attacks is usually **not to infect a computer** or computer system, or to **overcome security protection with a password** that protects it, but to **either overwhelm or temporarily disable it** using a series of repeated requests. Typically, this will restrict or block access to services.

In order to be able to legally prosecute an "attacker" who has used DoS or DDoS attacks, it is necessary to determine whether **his conduct was illegal** and, if so, how serious the conduct was. The point is that a DDoS attack in its nature can be, for example, the completely above board activity of Internet users trying to connect at one time (in a short period of time) to a web server of a company that provides discounts on tickets and, for example, announced that from 12.00 there will be a comprehensive reduction of tickets by 75%. Or it may be access by a large number of users to a web service of one of the popular media that report on important or newsworthy events – the inauguration of a new president, the death of a prominent person, etc. If the target computer system (webserver) is insufficiently dimensioned or is incorrectly configured (it is not able to handle the required amount of access), it will "collapse" similarly to a targeted DDoS attack. The question then is whether users who tried to log in to said website at the given time and thus practically caused the shutdown of the service in question should be punished.

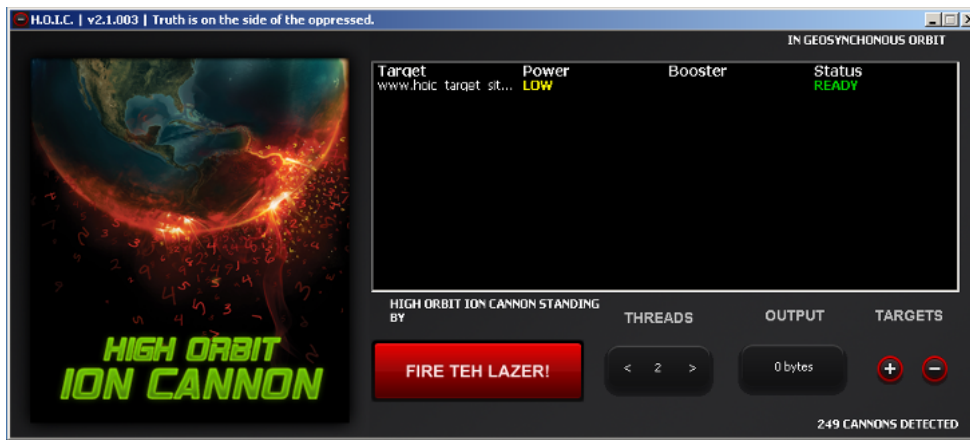
I believe that in the cases outlined above, although users have caused a massive DDoS attack on a provider's service, it is not realistic or even conceivable to punish these "pseudo-attackers" by any legal instrument, as their conduct was not illegal from the outset.

However, a different case would be a situation where attackers are called, for example, via the Internet and at a specific time, due to their re-login to the provided service, suppress this service. [4] Such cases occurred, for example, in the context of protests against the ACTA (Anti-Counterfeiting Trade Agreement) in 2012, when one of the options for committing these attacks was to use a tool distributed to Anonymous supporters, the LOIC (Low Orbit Ion Cannon).



LOIC (Low Orbit Ion Cannon) [5]

The imaginary successor of LOIC was the HOIC (High Orbit Ion Canon) software, which was developed as a replacement for LOIC.



### HOIC (High Orbit Ion Canon)\_[6]

The conduct of the attackers in this case is certainly illegal, because these attackers were aware or at least understood that their actions interfere with the rights of others. In this case, it would be possible to use the instruments of criminal, administrative and civil law.

Due to the adoption of the Convention on Cybercrime, criminal law should be harmonised and such legal norms should be adopted, in the EU member states and beyond, which should be able to punish DoS or DDoS attacks by the criminal law of that country. The following calls for protection against these attacks and the implementation of legislative measures: Chapter II – Measures to be taken at national level, Section 1 – Offences against confidentiality, integrity and usability of computer data and systems, Article 4 – Interference with data, of the Convention:

1. *Each Party shall take such legislative and other measures as may be necessary to establish as a criminal offence, in accordance with its domestic law, an intentional unlawful damage, erasure, deterioration, alteration or **suppression of computer data**.*
2. *A party may reserve the right to stipulate that it will consider the conduct described in paragraph 1 to be criminal only if it causes serious harm.*

### Possibilities of criminal sanctions in the Czech Republic

It follows from the wording of the provisions of **Section 230 (2)** (Unauthorised access to the computer system and information carrier) of the Criminal Code:

**Whoever gains access to a computer system** or information medium and

- a) uses data stored in a computer system or information media without an authorisation,
- (b) erases or otherwise destroys, damages, modifies, **suppresses**, or corrupts the quality of **data** stored in a computer system or information media, or renders them unusable without authorisation...

It follows from this provision that an attacker committing a DoS or DDoS attack must, in order to be criminally liable, **gain unauthorised access to a computer system and subsequently suppress the data in it**\_[7]

In this case, two separate articles (Chapter II, Section 1, **Article 2 – Illegal Access** and **Article 4 – Interference with data**) of the Convention on Cybercrime were merged into one provision.

The legislator thus made it practically impossible to punish the perpetrators of DoS or DDoS attacks by means of criminal law, as an offender is required to **gain unauthorised access to the computer system**. This legal interpretation, which requires gaining unauthorised access to a computer system, thus allows an offender to be punished only for the conduct specified in the Convention on Cybercrime in **Article 2 – Illegal Access**: “Each Party shall take such legislative and other measures as may be necessary to ensure that, under its domestic law, **unauthorised access to all or any part of a computer system** is a criminal offence when committed intentionally.”

From a technical point of view, DoS or DDoS attacks do **not** gain access to a computer system or part of it, or at least it is not the primary goal.\_[8]

For the above reasons, I am convinced of the need to incorporate into the Czech legislation a separate objective element of the crime, which would protect the computer system from DoS, DDoS, DRDoS, etc. attacks and which would respect the provisions of the Convention on Cybercrime. It would be possible to use, for example, the following wording:

**“Whoever prevents the use of a computer system without authorisation...”**

At present, it would be theoretically possible to charge perpetrators with DoS and DDoS attacks for a criminal offence under **Section 228** (damage to property) of the Criminal Code.\_[9] However, a condition for the use of the institution of damage to property would have to be the fact that such a thing (including a computer system) would be destroyed, damaged or made unusable. However, this condition usually only applies to this type of attack with regard to a certain temporary unusability.

In this context, however, the question also arises as to how and which way the actual damage will be quantified in the event of damage to a thing and who will be liable.\_[10]

Other objective elements that an attacker committing a DoS and DDoS attack could commit in certain circumstances include Section 272 (General threat), Section 273 (General threat due to negligence) of the Criminal Code.

Regarding the possible criminal sanction of a perpetrator of DoS or DDoS attacks, it is also important to determine (identify) the offender of this particular crime. The question remains as to **who should be criminally prosecuted as the offender** who, for example, caused the unavailability of a certain service (e.g. web application).

### Possibilities of criminal sanctions in Poland

In this case, Article 268 of the Criminal Code is applicable, stating that:

§ 1. Whoever, without being authorised to do so, destroys, damages, deletes or alters a record of essential information or otherwise prevents or considerably hinders an authorised person from becoming acquainted with it, shall be subject to a fine, the penalty of restriction of liberty or deprivation of liberty for up to 2 years.

### Possibilities of criminal sanctions in Portugal

Such acts are clearly under the scope of Computer sabotage [Illegal interference] (Art. 5(1) of Cybercrime Law), possibly as aggravated offence in the case of high damage or interfering with critical infrastructures or other essential services (Art. 5(5)).

[1] For more details, e.g. MARCIÁ-FERNANDÉZ, Gabriel, Jesús E. DÍAZ-VERDEJO and Pedro GARCÍA-TEODORO. Evaluation of a Low-rate DoS Attack Against Application Servers. *Computers & Security*, 2008, vol. 27, No. 7–8, pp. 335–354.

CARL, Glenn, Richard BROOKS and Rai SURESH. Wavelet Based Denial-of-Service Detection. *Computers & Security*, 2006, vol. 25, No. 8, pp. 600–615

RAK, Roman and Radek KUMMER. Informační hrozby v letech 2007–2017. *Security magazin*, 2007, vol. 14, No. 1, pp. 3.

[2] For example, DoS attacks on the websites of the presidency, parliament, ministries, media outlets and two Estonian banks – Estonia (2007). *Estonia recovers from massive DDoS attack*. [online]. [cit. 4. 3.2010] Available from: [http://www.usatoday.com/tech/news/techpolicy/2007-09-12-spammer-va\\_N.htm](http://www.usatoday.com/tech/news/techpolicy/2007-09-12-spammer-va_N.htm)[http://www.computerworld.com/s/article/9019725/Estonia\\_recovers\\_from\\_massive\\_DDoS\\_attack](http://www.computerworld.com/s/article/9019725/Estonia_recovers_from_massive_DDoS_attack)

[3] At this point it is necessary to mention **Handshake** – a process whose task is to set the parameters of a communication channel between two subjects before starting the actual communication. For example, a handshake is used on the Internet to open a TCP connection (the so-called “**three-way handshake**”, i.e. an exchange of three datagrams), and only then does the actual data transfer follow. Three separate steps are required to establish a TCP connection:

1. **A party initiating the connection (client) sends a TCP segment with the SYN flag set.**
2. **A receiving party (server) responds with a TCP segment with the SYN + ACK flags set.**
3. **The client responds with a TCP segment with the ACK flag set.**

Other TCP segments already have only the ACK flag set.

For more details, see e.g. *TCP handshake krok za krokem*. [online]. [cit.18.8.2016]. Available from: <http://www.svetsiti.cz/clanek.asp?cid=TCP-handshake-krok-za-krokem-3122000>

There are other ways of DoS attack, e.g. “TearDrop”, “Nuke”, “Peer-to-Peer attack”, etc. For more details cf. [online]. [cit.25.9.2010]. Available from: [http://cs.wikipedia.org/wiki/Denial\\_of\\_Service](http://cs.wikipedia.org/wiki/Denial_of_Service)

[4] It can also be a case where an attacker sends a hoax of type “on 6 June 2016 from 12 to 13, tickets will be free at Lufthansa! Click here for more information.”

[5] *LOIC*. [online]. [cit.18.8.2016]. Available from: <https://i.ytimg.com/vi/QAbXGy0HbrY/maxresdefault.jpg>

[6] *HOIC*. [online]. [cit.18.8.2016]. Available from: <https://npercoco.typepad.com/a/6a0133f264aa62970b0167612ea130970b-pi>

[7] Suppression means the activity listed in Article 4 of the Convention on Cybercrime.

[8] If, for example, a PING flood is used for a DoS or DDoS attack, then it is possible to imagine the whole situation as the constant calling (and subsequent hanging up) to a specific telephone number. This will lead to a situation where the attacked phone number does not have the ability to make its own call (the call function is blocked), but none of the callers (attackers) will receive any data stored in the attacked phone.

[9] See Section 228 (1) of the Criminal Code:

“Whoever destroys, damages or renders useless another’s possession and thus causes damage not insignificant to another’s property, shall be sentenced to imprisonment for up to one year, to prohibition of the activity or to forfeiture of a possession or other asset of value.”

Damage not insignificant means damage amounting to at least CZK 5,000 (see Section 138 (1) of the Criminal Code)

[10] Will every attacker be held accountable for this damage? Will responsibility for this damage be “divided” among the attackers?

## 4.14. Dissemination of defective content

Currently, two basic types of defective content dissemination can be described. **Dissemination of prohibited types of pornography and dissemination of hateful and extremist content.**

In the case of the dissemination of **prohibited types of pornography**, it is mainly the dissemination of pornographic material depicting contact with animals and the dissemination (or possession) of "child pornography" (material depicting or otherwise using a child – a person under the age of 18, or a person who appears to be a child). There are countless methods of distribution. From simply offering this type of pornography for download to placing this material on the Internet, distributing it via exchange computer networks, sending them via e-mail, etc.

Most countries in the world have committed themselves to prosecuting child abuse leading to the production of pornographic material and the subsequent distribution of such material, whether or not they have ratified the Cybercrime Convention. Although considerable activity is being developed in this area (not only by states, non-profit organisations and others), the problem of child sexual abuse online persists.

The phenomenon of child pornography has co-existed with society from the first moments when it was possible to capture an abusive act on any medium (paper, film, etc.). However, the truth is that the Internet has allowed the mass dissemination of such materials among individual users, as well as their greater degree of anonymity.

The problem of the Internet and cyberspace is related to the previously stated statement that *"the Internet does not forget"*. If any material is uploaded or transmitted via ICT, there may always be a copy of that material somewhere. An example from the Czech Republic, where users themselves create material that depicts naked children, can be the file hosting portal [www.rajce.net](http://www.rajce.net). This portal has certainly not been created as an environment for the distribution of any pornographic or otherwise harmful material (there are other sites for this purpose), but users do not respect the basic rules of the rajce.net service, especially Article 13, which states:

*"Content depicting naked people, especially those under the age of 18, may only be placed on private albums with a password on Rajce; the other provisions of these rules, in particular the prohibition on placing pornographic content or content unlawfully infringing on the right to the protection of the personality of third parties, shall remain unaffected in such a case."*

Nevertheless, it is possible to find a number of photographs on this site, albeit created with good intentions (for example, a sharing of photographs among family members living far apart), which are attractive to anyone, including a potential attacker. Due to other information that is published on this portal, or due to the correlation of data from other sources available online, it is much easier for an attacker, for example, to find a potential victim.

The problem is not the uploading of photos of naked people (with the knowledge of data replication), but the fact that this data is open to all users, not just a narrowly limited group (e.g. the already mentioned family).



**A photo from rajce.net (photo is freely available to all users)**

In conclusion, I want to say that I definitely have nothing against taking pictures of children (or sharing some photos with immediate family) because of the preservation of beautiful memories. What bothers me is the stupid and careless way these photos are made available to anyone in cyberspace.

One recent project dealing with online child abuse was the work of the Dutch company Terre des Hommes Netherlands (THN). This company created a virtual ten-year-old Filipino girl **Sweetie**. Sweetie communicated on Internet chats for ten days and was approached by approximately twenty thousand men. A thousand of them offered her money in exchange for online sex.

Project chief Hans Guyt told a news conference in The Hague that this type of crime required a new way of police work. *"Predators and their victims will not approach us during the investigation,"* he said.

*"We created a virtual identity in the form of a ten-year-old Filipino girl."*

"We didn't attract anyone until they offered us money," Guyt said.

In this way, the activists wanted to draw attention to the growing problem of child abuse through webcams. They call this phenomenon "Internet sex tourism."<sup>[1]</sup>

### Possibilities of criminal sanctions in the Czech Republic

In the case of creation, possession or distribution of materials falling under the term child pornography, it is possible to penalise the user according to **Section 192** (Production and other handling of child pornography), **Section 193** (Child abuse to produce pornography) of the Criminal Code. Participation in a pornographic performance or other similar performance in which a child performs is also a criminal offence (**Section 193a** of the Criminal Code). It is also a criminal offence to gain access to child pornography through information or communication technology (**Section 192 (2)** of the Criminal Code).

It is also a criminal offence where a user has produced, imported, exported, transported, offered, made publicly available, brokered, put into circulation, sold or otherwise provided a photographic, film, computer, electronic or other pornographic work in which violence or disrespect for a person, or which describes, depicts or otherwise depicts sexual intercourse with an animal (**Section 191 (1)** of the Criminal Code).

In the case of a **dissemination of hateful and extremist content**, a criminal offence mainly includes the support and promotion of a movement that is demonstrably aimed at suppressing human rights and freedoms, expressions of sympathy with such a movement, proclamation of racial, ethnic and national, religious or class resentment or resentment against another group. It also includes the spread of defamation by means of information technology and, last but not least, the sending of annoying messages falling under the concept of stalking or cyberstalking.

In these cases, there may be a number of crimes, such as **Section 184** (Defamation), **Section 353** (Dangerous Threatening), **Section 354** (Dangerous Pursuing), **Section 355** (Defamation of Nation, Race, Ethnic or other Group of People), **Section 356** (Instigation of Hatred towards a Group of People or of the Suppression of their Rights and Freedoms), **Section 403** (Establishment, Support and Promotion of Movements Aimed at Suppression of Human Rights and Freedoms), **Section 404** (Expressing Sympathies for Movements Seeking to Suppress Human Rights and Freedoms), **Section 405** (Denial, Impugnation, Approval and Justification of Genocide) of the Criminal Code.

### Possibilities of criminal sanctions in Poland

In Poland the following Article of the Penal Code apply:

Art. 200b. Public promotion of paedophilic content

Art. 202. Presentation and distribution of pornography

### Possibilities of criminal sanctions in Portugal

Such acts are criminalised in different ways, depending on the case. First of all, they may be considered as Offences related to child pornography (Art. 176 of the Criminal Code). On the other hand, they may be an Aggravated breach of privacy (Arts. 191(1)(b) and 197(b) of the Criminal Code) or as Revenge pornography related to domestic violence (Art.152(2)(b) of the Criminal Code (Art. 193() of the Criminal Code).

Besides, the objective elements of crimes like Discrimination and incitement to hate and violence (Art. 240 of the Criminal Code) or Defamation (Art. 180 of the Criminal Code) might be present.

---

<sup>[1]</sup>For more details see:

Computer-generated 'Sweetie' catches online predators. [online]. [cit.19.8.2016]. Available from: <http://www.bbc.com/news/uk-24818769>

Nizozemci vytvořili virtuální dívku. Pomohla lapit přes tisíc pedofilů. [online]. [cit.19.8.2016]. Available from: [http://zpravy.idnes.cz/virtualni-holcicka-pomohla-lapit-tisic-pedofilu-fuu-zahranicni.aspx?c=A131106\\_210025\\_zahranicni\\_zt](http://zpravy.idnes.cz/virtualni-holcicka-pomohla-lapit-tisic-pedofilu-fuu-zahranicni.aspx?c=A131106_210025_zahranicni_zt)

Video with **Sweetie** is available online: <https://www.youtube.com/user/sweetie>.

## 4.15. Cyberattacks on social networks

Bullying in the real world consists in the attempt of an attacker to harm, humiliate, ridicule or insult another, whether physically or mentally. Cyberbullying then transmits "classic bullying" into the virtual world and allows an attacker to use tools and resources that can have a much greater impact on the victim than would be the case in the real world. Cyberbullying, through the use of information and communication technologies and the durability of data in cyberspace, allows for repeated attacks on a victim, even if the victim has geographically moved far away in the real world from where he/she was originally bullied.

Cyberbullying can be linked to "classic" bullying (e.g. recording a victim's physical assault and then posting the attack on the web). In order to talk about cyberbullying, it is necessary to use information and communication technologies or services offered in cyberspace for bullying.

### The signs of cyberbullying include:

- **Feeling anonymous** (Attackers usually feel that they cannot be traced due to the Internet.)
- **Unlimited attack** (Due to ICT, attackers do not have to deal with the time or space for their attack. It is possible to bully at any time, from anywhere and anyone. Such an attack also requires much less effort than in the case of "classic" bullying.)
- **Unlimited group of attackers** (Unlike the real world, in the virtual world it does not matter the age, gender, physical strength, position of the attacker in the group, etc. Any person can be a bully.)
- **Unlimited space and resources** (The Internet provides an attacker with practically unlimited space and resources for bullying. An attacker can repeatedly post offensive remarks, photo and video comments on various portals, social networks, etc. He/she can improve and "refine" these materials.)
- **Difficult to detect** (Unlike classic bullying, cyberbullying may not have external manifestations such as bruising, missing money, etc.)
- **Persistence** [Classic bullying usually consists of individual attacks, which are repeated, but the single attack for the victim always ends. For cyberbullying, for example, one SMS, e-mail, etc. is enough, a victim keeps coming back to them (respectively, they are constantly reminded, sent, etc.), so he/she can live in trauma for months. Offensive SMS, e-mails, photos, etc. are more permanent than individual physical attacks.]

### The most common manifestations of cyberbullying:

1. Gossip, intimidation, insult, ridicule or other embarrassment (social networks, e-mail, SMS, chat, ICQ, Skype, games, etc.).
2. Acquisition of sound recordings, videos or photographs, their graphic or other editing and subsequent publication in order to harm (ridicule) a selected person.
3. Filming of videos in which a victim is physically attacked or otherwise mentally abused and ridiculed. These videos are then published online (this is called Happy Slapping).
4. Creating websites, social accounts (modifying original or creating new profiles), discussion portals, etc. that insult, slander or humiliate a specific person.
5. Misuse of another's account – identity theft (e-mail, discussion, etc.).
6. Provoking and attacking users in discussion forums (chat rooms, etc.).
7. Uncovering other people's secrets.
8. Blackmail using a mobile phone or the Internet.
9. Harassment and pursuing by calling, writing messages or ringing.

### Consequences of some attacks:

- **Amanda Todd** (15 years old). Amanda's story can be found in her own video available at: [http://www.youtube.com/watch?v=qDIKB2\\_RpuY](http://www.youtube.com/watch?v=qDIKB2_RpuY). Amanda committed suicide.
- **Rebecca Ann Sedwick** (12 years old) was bullied on the Internet for almost a year. She committed suicide in 2013. The bullying began after Rebecca had been dating a boy for some time. Her mother told reporters that her daughter had been receiving messages like: 'You're disgusting,' 'Why are you still alive?' and 'Go kill yourself'. The situation escalated so much that the mother dropped her daughter out of Crystal Lake school and cancelled her Facebook account. She reportedly had to leave school. The mother taught her at home for the rest of the year. She joined another school in September. Everything seemed to be getting better and Rebecca cheered up in the new school. But she secretly signed up for new applications, including Kik Messenger and Ask.fm telephone messaging, and the bullying began again after she had begun inquiring about being overweight on the Internet. Sheriff Judd said the girl had been "completely terrorised" on social media.
- **Ghyslain Raza** (14 years old, Canada), known as the Star Wars Kid. <https://www.youtube.com/watch?v=HPPj6vilBmU&spfreload=10>. Ghyslain Raza filmed himself performing a battle scene from Star Wars. He tried to imitate the character of Darth Maul. His classmates stole the recording and published it on the Internet to entertain others. Within a few weeks, the recording flew around the world, was modified many times, and a number of websites and blogs were created, on which the boy was ridiculed. Ghyslain's fans wrote a petition to the Star Wars creators to cast him in one of the episodes. He was even parodied in some series (e.g. South Park, American Dad, Veronica Mars). Ghyslain had a mental breakdown and had to be treated for a long time.



- **Anna Halman**(14 years old, Poland). Five classmates subjected Anna to sexual bullying in front of the whole class. (They took off her clothes and pretended to rape her.) They recorded the whole scene on a mobile phone and threatened the girl that they would publish the recording on the Internet. They also did so later, posting the video on YouTube. It was supposed to be revenge for Anna for not wanting to date one of the boys. Anna committed suicide.
- **Jessica Logan** (18 years old, USA). After their breakup, Jessica's ex-boyfriend published her intimate photos, which she had sent him while they were still dating. Jessica was then exposed to constant ridicule from her classmates. The attacks on her intensified after she had appeared anonymously on television to warn others about the risks of sexting. Jessica committed suicide.

### Possibilities of criminal sanctions in the Czech Republic

Cyberbullying (like classic bullying) is not in itself a crime or an offence. It always depends on the actions of the bully. If such an action was a form of, for example, physical harm to a victim, blackmail or intimidation, then the application of, for example, **Section 146** (Bodily Harm) or **Section 145** (Grievous Bodily Harm), **Section 175** (Extortion) of the Criminal Code could be considered. In the case of harassment and pursuing of a person, it would be possible to use the provisions of **Section 354** of the Criminal Code (Dangerous Pursuing). However, in the case of cyberbullying, which can be manifested in, for example, constant ridicule, embarrassment and psychological harm through information and communication technologies, the application of some of the above provisions will be problematic, if not impossible.

### Possibilities of criminal sanctions in Poland

In Poland this is regulated by:

Art. 212 kk – Defamation

and

Art. 190 § 1. Whoever threatens another person with committing a criminal offence to his/her detriment or to the detriment of a person close to him/her, if the threat induces in the person threatened a reasonable fear that the threat will be carried out, shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to 2 years.

§ 2 Prosecution shall occur on the motion of the injured person.

### Possibilities of criminal sanctions in Portugal

As such, cyberbullying is not a criminal offence. However, it may be considered as a form of Persecution (Art. 154-A of the Criminal Code), but also as Sexual Harassment, an Insult, a Defamation, an Aggravated breach of privacy or even as Discrimination and incitement to hate and violence (Arts. 170, 181, 180, 192 and 197(b) and 240, all the of the Criminal Code).

## 4.16. Identity theft

Identity theft is an attack in which a virtual identity is stolen<sup>[1]</sup>, or it is a takeover of control (permanent or temporary) of this identity. The motive for an attacker's actions may be financial gain, but also other benefits, such as access to information about other people, access to company data, etc., which are associated with the fact that an attacker acts on behalf of another person.

The actions of an attacker usually consist of several illegal actions at once. The first crime in identity theft is hacking into access data or installing malware on a victim's computer system in order to gain access to a virtual identity.

After gaining access to an identity of an attacked person, the information obtained may be misused to attack this person and the identity may be misused to attack another person. An attack on another victim through a stolen identity is much easier for an attacker because this second victim by default has no information about changing the identity of the person (the first victim), with whom, for example, regularly communicates and exchanges sensitive data.

If I return to the issue of botnets in this context, one of the typical tasks of malware that is installed when a computer system is connected to a botnet network is the automatic extraction of data about users of the infected computer system – i.e. identity theft. Botmaster can then use the obtained data at any time by impersonating a certain person or selling this data to third parties.<sup>[2]</sup>

Typically, stolen identities are used to:

- carrying out phishing or malware attacks within the list of users with whom a person with a stolen identity communicates,
- sending spam,
- obtaining information that is not publicly available (for example, information on the structure of a company, security settings for other services, etc.),
- gaining access to other services. Many online services allow you to change your password just by entering your e-mail address. Due to the fact that an attacker controls an e-mail box of an attacked person, the access data can be changed in a number of other services that are associated with this e-mail box.

### Possibilities of criminal sanctions in the Czech Republic

If a security measure is overcome and unauthorised access to a victim's identity is obtained, the features of the crime according to **Section 230 (1)** (Unauthorised Access to Computer Systems and Information Media) of the Criminal Code will be fulfilled. When using malware for the same purpose, an attacker commits an act under Section 230 (2) of the Criminal Code. If the aim of identity theft is to obtain an unjustified benefit for oneself or another, it is also possible to apply the provisions of **Section 230 (3)** of the Criminal Code. In the event that an attacker steals an identity with the aim of deceiving another, i.e. misleading somebody in order to enrich himself/herself, such conduct could also be assessed in accordance with **Section 209** (Fraud) of the Criminal Code.

### Possibilities of criminal sanctions in Poland

Pursuant to Art.190a § 2 of the Penal Code anyone who, impersonating another person, uses his image or other personal data in order to inflict material or personal damage on him faces a penalty of up to three years imprisonment.

### Possibilities of criminal sanctions in Portugal

Pretending to be someone else is no longer criminalised. However, the creation of inauthentic data for legally relevant purposes would be considered as aComputer-related forgery (Art. 3 of the Cybercrime Law). Besides, being the purpose of such impersonation a fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person, on the expenses of the victim, it would also be considered as aComputer-related fraud (Art. 221(1) of the Criminal Code).

---

[1] Virtual identity means any identity or avatar used by a person to interact within cyberspace (e.g. e-mail, social network account, a game, in various online marketplaces, within a computer system, etc.). It does not matter whether a virtual identity is true or false, i.e. whether it represents a real person, or it is a completely artificially created identity, without a real basis.

[2] For more details see: PLOHMANN, Daniel, Elmar GERHARDS-PADILLA and Felix LEDER. *Botnets: Detection, Measurement, Disinfection & Defence*. ENISA, 2011, p. 22 [online]. [cit.17.5.2015]. Available from: <https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence>

## 4.17. APT (Advanced Persistent Threat)

APT means an advanced and persistent threat. It is a long-term systematic cyberattack, focused on a target computer system, or on the ICT of a target organisation. Various techniques and relatively large resources are used for such an attack, and typically secondary targets (e.g. computer systems such as repeated DoS or other attacks) can be attacked in order to divert attention from the primary target (malware infiltration of a company), which is then attacked.

*"APT is usually focused on extracting strategically valuable classified or non-public data, limiting a target's ability to act, or taking a position that enables the future implementation of the above-mentioned. The implementation of actions that meet the definition of APT is associated with a high level of expertise, considerable financial resources and the ability to adapt to the actions of the victim of the attack in the long term. The character of APT thus acquires primarily state actors, i.e. their controlled and sponsored groups, or specialised groups of organised crime."*[1]

An APT attack typically consists of:

- an acquisition of information about a target of an attack (collection of information from open sources; use of social engineering, etc.)
- an actual attack:
  - o Selection of suitable means (malware, creation of cover identities, etc.)
  - o If a system is vulnerable from the outside, it is attacked
  - o If a system is inaccessible from the outside, other techniques combined with social engineering are used (e.g. Spear phishing, Identity Theft, etc.)
- taking control of some computer systems, consolidating positions within the compromised computer network
- collecting data and information and sending them to the attacker
- data extraction

During an APT attack, attackers can use other different types of attacks on the selected target, depending on the data and information they have acquired.

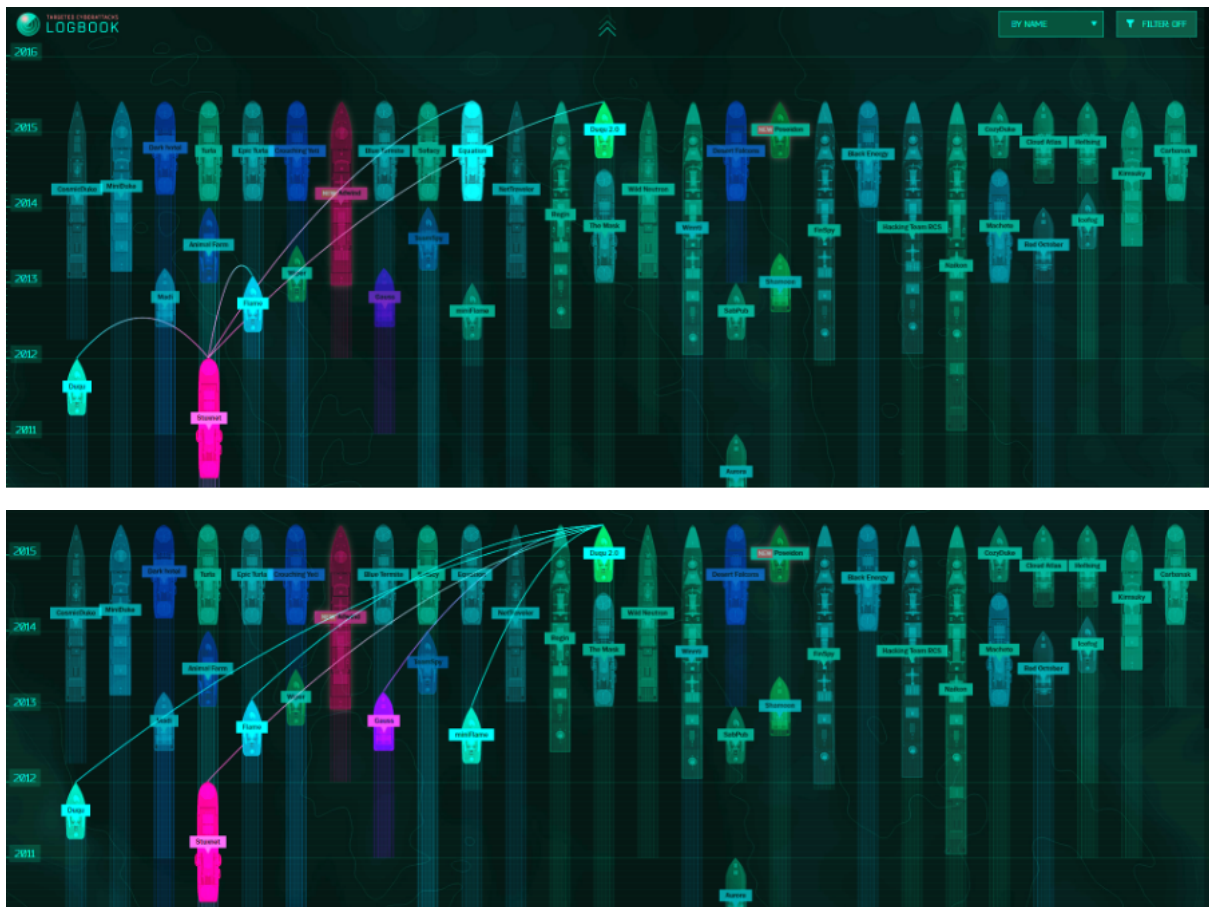
APT can be displayed using its life cycle:



Life cycle of APT attack.[2]

An APT attack can last from several months to many years, and an attack can include relatively long periods when the activity of attackers is minimal. It is no exception to conduct a large number of similar operations against different objectives at the same time.[3]

The Kasperky Lab website (<https://apt.securelist.com/#firstPage>) visually depicts known APT attacks, including information on when a sample of attack malware first appeared, when an APT attack was discovered, where it primarily operates (geolocation information, primarily attacked operating systems, number of targets, etc.), etc. The following two print screens show the primary binding of Stuxnet malware (including, among others, to Duqu 2.0) and then the binding of Duqu 2.0 to other malware.



Display of APT attacks including their interconnection.[4]

### Possibilities of criminal sanctions in the Czech Republic

Any criminal sanction of an attacker or attackers performing an APT attack then depends entirely on their actions, which may take the form of, for example, distribution of malware, one of the phishing attacks, Identity Theft, etc.

### Possibilities of criminal sanctions in Poland

When analysing an APT attack in terms of violations of the law in force in Poland, it should be considered that if an attack was carried out at all its stages, at least a few offences would be committed. Pursuant to the applicable legal regulations, an APT attack may be considered:

- hacking under Art. 267 § 1 of the Penal Code
- crime of producing or making available computer devices or programs, passwords and codes under Art. 269 b of the Penal Code
- computer fraud under Art. 287 of the Penal Code

Other crimes that may occur during the implementation phase are:

- computer sabotage under Art. 269 of the Penal Code,
- bringing danger to life, health or property under Art. 165 of the Penal Code,
- destruction, damage, deletion of IT data from art. 268 a of the Criminal Code,
- disruptions in the operation of the computer system or ICT network pursuant to Art. 269a.

An APT attack can also be tantamount to espionage under Art. 130 § 3 of the Penal Code.

### Possibilities of criminal sanctions in Portugal

APT attack aren't specifically criminalised, not even as aggravated offences.

[1] *Advanced Persistent Threat*. [online]. [cit.20.8.2016]. Available from: <https://www.isouvislosti.cz/advanced-persistent-threat>

[2] *Advanced Persistent Threat – life cycle*. [online]. [cit. 20. 8. 2016]. Available from: [https://upload.wikimedia.org/wikipedia/commons/7/73/Advanced\\_persistent\\_threat\\_lifecycle.jpg](https://upload.wikimedia.org/wikipedia/commons/7/73/Advanced_persistent_threat_lifecycle.jpg)

[3] For more details see: *Advanced Persistent Threat*. [online]. [cit. 20. 8. 2016]. Available from: <https://www.isouvislosti.cz/advanced-persistent-threat>

*Advanced Persistent Threat (APT)*. [online]. [cit. 20. 8. 2016]. Available from: <http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT>

*Advanced Persistent Threats: How They Work*. [online]. [cit.10.7.2016]. Available from: <https://www.symantec.com/theme.jsp?themeid=apt-infographic-1>

*How do APTs work? The Lifecycle of Advanced Persistent Threats (Infographic)*. [online]. [cit. 10. 7. 2016]. Available from: <https://blogs.sophos.com/2014/04/11/how-do-apt-work-the-lifecycle-of-advanced-persistent-threats-infographic/>

[4] *Targeted cyberattacks logbook*. [online]. [cit.10.7. 2016]. Available from: <https://apt.securelist.com/#secondPage>

## 4.18. Cyberterrorism

In connection with cyberattacks, we cannot neglect to mention terrorism, which is one of the current global threats, or its noticeable dynamic growth and spread worldwide.

Terrorism can be divided according to form into *lethal* and *non-lethal* forms, where the first group is characterised by the use of common means of violence (*conventional* – attacks committed using commonly available weapons, such as firearms and unconventional – misuse of weapons of mass destruction). However, **non-lethal forms of terrorism**<sup>[1]</sup> or attacks using more modern tools in combination with lethal means are more common in the Internet.

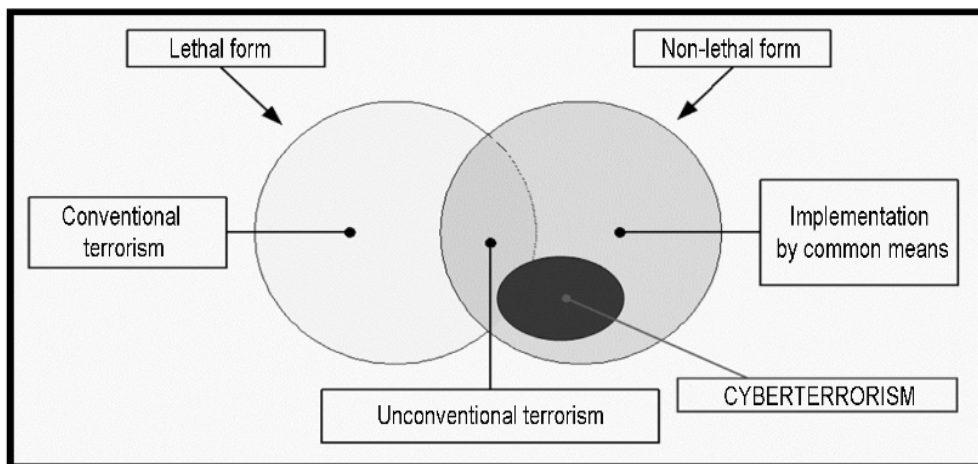
The conventional form of non-lethal terrorism includes the following subgroups:

- *Unarmed terrorism*.

- *Cyberterrorism*, one of the greatest dangers of the 21st century. The principle is primarily the misuse of ICT (including the Internet) as a means and environment for carrying out an attack. Similarly to the classic conventional terrorist attack, this is a planned activity usually politically or religiously motivated and carried out by small rather than militarily organised structures. The aim of these groups is primarily to influence public opinion. Due to the rapid spread of information and communication technologies around the world, cyberterrorism poses a significant threat and is increasingly used by terrorist groups.<sup>[2]</sup>

- *Media terrorism*, in which there is a planned abuse of the media and other psychological weapons in order to influence the opinions of the entire population or target groups of the population.

This relationship is most aptly characterised by the diagram shown in the following figure.



**Forms of terrorism, including cyberterrorism**

The global nature of the IT and telecommunications environment enables the transfer of information and the coordination of terrorist activities throughout the world. It is stated that, for example, the attack on the WTC in New York was organised using the Internet.

There may be other cases of misuse of the Internet for the dissemination of malicious information or for psychological operations related to media terrorism. The Internet plays a significant role in spreading propaganda, ideology or intimidation, for example by publishing executions of prisoners online<sup>[3]</sup>, attracting and mobilising new activists, sympathisers or sponsors, defending terrorist acts and inciting individuals to commit them. Terrorist groups' Internet sites often contain instructions for making makeshift weapons, or propaganda targeted at the younger generation.

The Internet provides exceptional opportunities for extremist and terrorist groups as well as individuals, especially in the area of fast and relatively secret communication, where it serves to exchange information and instructions for planning and coordinating events or transferring funds.

Almost all terrorist groups and organisations run their websites. They are usually published in several language versions, and there are also special pages aimed at children and women containing fairy tales or comics, which incorporate, for example, the stories of suicide bombers.<sup>[4]</sup>



TravelWest.info website after being attacked by attackers

### Possibilities of criminal sanctions in the Czech Republic

From the point of view of criminal law, the aforementioned acts may fulfil the objective elements of criminal offences under **Section 311(2)** (Terrorist Attack), **Section 355** (Defamation of Nation, Race, Ethnic or other Group of People), **Section 356** (Instigation of Hatred towards a Group of People or of the Suppression of their Rights and Freedoms), **Section 364** (Incitement to Criminal Offence), **Section 403** (Establishment, Support and Promotion of Movements Aimed at Suppression of Human Rights and Freedoms) and **Section 404** (Expressing Sympathies for Movements Seeking to Suppress Human Rights and Freedoms) of the Criminal Code.

### Possibilities of criminal sanctions in Poland

In Poland, Articles 265 through 269 and Article 287 of the Penal Code apply to the implementation of a cyberterrorist attack and, depending on the effect of the cyberterrorist attack, some other Articles of the Penal Code may also be applicable, such as:

Art. 163 Causing a catastrophe

Art. 164. Causing the danger of a catastrophe

Art. 165. Causing public danger

Art. 173 Causing a traffic accident

Art. 174. Causing an imminent danger of a traffic disaster

### Possibilities of criminal sanctions in Portugal

According to Law No. 52/2003, on the fight against terrorism, if connected with terrorism intents, the penalties for offences such as Computer-related fraud or Computer related forgery will be aggravated by a third (Art. 4(2)). Besides, the public provocation to offences related to electronic communications (Art. 4(3)(4)), recruiting (Art. 4(5)(6)) or the promotion of terrorist groups or actions are aggravated if practiced by the Internet (Art. 4(8) (9)).

[1]\_However, it is possible to imagine a combination of these attacks. For more details, see e.g.:

*Exclusive: Computer Virus Hits U.S. Drone Fleet.* [online]. [cit.10.7.2016]. Available from: <https://www.wired.com/2011/10/virus-hits-drone-fleet/>

[2]\_JIROVSKÝ, Václav. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Prague: Grada, 2007, p. 129

[3]\_The presented URL is not censored and contains drastic footage! See e.g.:

*WATCH: ISIS Downs Prisoners Alive & Blows Hostages Up With RPG & Kills Others With Explosives – Graphic video.* [online]. [cit.20.8.2016]. Available from: <https://www.zerocensorship.com/uncensored/isis/drowns-prisoners-alive-blows-hostages-up-with-rpg-kills-others-with-explosives-graphic-video-132382>

*Disturbing ISIS video shows militants beheading four prisoners and gunman executing shoppers at market.* [online]. [cit.20.8.2016]. Available from: <http://www.mirror.co.uk/news/world-news/disturbing-isis-video-shows-militants-7306017>

[4]\_JIROVSKÝ, Václav. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Prague: Grada, 2007, p. 138

See also e.g.:

*Cyber Terrorism: How Dangerous is the ISIS Cyber Caliphate Threat?* [online]. [cit.20.8.2016]. Available from: <http://www.govtech.com/blogs/lohrmann-on-cybersecurity/Cyber-Terrorism-How-Dangerous-is-the-ISIS-Cyber-Caliphate-Threat.html>

*Islamic State Hacking Division*. [online]. [cit.20.8.2016]. Available from: [https://ent.siteintelgroup.com/index.php?option=com\\_customproperties&view=search&task=tag&bind\\_to\\_category=content:37&tagId=698&Itemid=1355](https://ent.siteintelgroup.com/index.php?option=com_customproperties&view=search&task=tag&bind_to_category=content:37&tagId=698&Itemid=1355)



## 4.19. SUMMARY



### SUMMARY / MAIN OUTPUTS FROM THE CHAPTER

- A significant part of cybercrime uses or transmits notorious types of illegal activities (such as fraud, copyright infringement, theft, bullying, etc.) to the digital environment, where they can be committed "better, faster and more effectively" than in the real world. Pure cyberattacks can include, for example, hacking, DoS and DDoS attacks, botnets, etc.
- With the development of services based on the principle of as-a-service, a number of platforms (typically underground, darknet forums) have emerged in the cybercrime environment, where services are offered that can be described as crime-as-a-service (cybercrime-as-a-service). Thus, a "malware or underground economy" emerges that provides almost any user with the means to commit cybercrime.
- The chapter introduces basic cyberattacks. A typical modus operandi is presented, as well as the possibilities of criminal sanctions for these actions.
- Cybercrime can be defined as conduct directed against a computer or, in some cases, computer network, or as conduct in which a computer is used as a tool to commit a crime. An indispensable criterion for the application of the definition of cybercrime is the fact that the computer network, or cyberspace, is then the environment in which this activity takes place.



### KEY WORDS TO REMEMBER

- social engineering
- botnet
- malware
- ransomware
- spam
- scam
- phishing
- pharming
- fraud
- hacking
- cracking
- DoS, DDoS
- APT



### KNOWLEDGE CHECK QUESTIONS

- What is characteristic for social engineering?
- What is a botnet and how does it work?
- What are the typical botnet topologies?
- Is it possible to criminalise an owner of a botnet?
- What is malware?
- What are the most common examples of malware?
- What are the most common malware infection vectors?
- What is ransomware and what are its manifestations?
- What is phishing and how is this attack most often conducted?
- What is the difference between phishing and pharming?
- What is hacking?
- What is characteristic for cracking?
- What is the difference between hacking and cracking?
- What is a DoS attack and how does it work?
- What is the difference between DoS and DDoS?
- What can be included in the distribution of defective content?

· What is APT?

## 5. Conclusion

I firmly believe that cyberspace must not become an environment where any crime can be committed with impunity. On the other hand, the rules and conditions need to be set so that it does not become an environment in which censorship and repression prevail. Balancing these two levels is a key prerequisite for applying and, in particular, respecting the rules in cyberspace, whether legal or moral.

With regard to the application of possible criminal law norms to certain types of cyberattacks, it should be noted that it is not possible to prosecute by criminal law such conduct, no matter how dangerous, that is not enshrined in the criminal codes of a country. Criminal law is an *ultima ratio* means and as such must be very precise so as not to interfere with the rights and freedoms of individuals to a greater extent than is strictly necessary.

In addition to the state, the protection of cyberspace and its users is handled by various private organisations. I believe that if we want to fight cybercrime effectively, there should be more effective cooperation of private organisations (especially IT experts, CSIRT teams, etc.) with public (state) administration, or with law enforcement authorities, so that it is possible to respond in a timely and adequate manner to increasingly sophisticated forms of cybercrime or cyberattacks.

As I mentioned in the introduction: *"Life without information and communication technologies is now inconceivable or impossible for our society."*

My view is that there is no point in getting rid of ICT and the services associated with these technologies. The purpose of this monograph was not to force users to uninstall Facebook and not use Google or other services. The purpose was to draw attention to the possible risks associated with the use of information and communication technologies and related services. In this context, it is necessary to recall the quote *Scientia est potentia* (**knowledge is power**). In the case of ICT and related services, it is necessary to know what these technologies and services represent, what they do and what they are used for.

The reduction of negative phenomena in cyberspace and the effort to change must necessarily begin with end users because in cyberspace it is they who are the typical first victim of an attacker. At the same time, users are an authority that can define what services, data or information will be searched, stored and provided in cyberspace.

I believe that the education and training of users should be an essential part of the penetration of information and communication technologies into our lives. Building information literacy should be inextricably linked to the creation, distribution and promotion of products or services that are associated with information and communication technologies. The actual education in this area, or rather learning about possible threats, risks and drawbacks posed by IT, should be part of the teaching of all forms of study at all levels of education.

*"Nobody made a greater mistake than he who did nothing because he could do only a little."*

Edmund Burke

## 6. Reference list

1. *10 Most Notorious Hacking Groups*. [online]. [cit.15.7.2016]. Available from: <https://www.hackread.com/10-most-notorious-hacking-groups/>
2. *7 Types of Hacker Motivations*. [online]. [cit.16.8.2015]. Available from: <https://blogs.mcafee.com/consumer/family-safety/7-types-of-hacker-motivations/>
3. *7 Types of Hackers You Should Know*. [online]. [cit.16.8.2015]. Available from: <https://www.cybrary.it/0p3n/types-of-hackers/>
4. *Advanced Persistent Threat – life cycle*. [online]. [cit. 20. 8. 2016]. Available from: [https://upload.wikimedia.org/wikipedia/commons/7/73/Advanced\\_persistent\\_threat\\_lifecycle.jpg](https://upload.wikimedia.org/wikipedia/commons/7/73/Advanced_persistent_threat_lifecycle.jpg)
5. *Advanced Persistent Threat (APT)*. [online]. [cit. 20. 8. 2016]. Available from: <http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT>
6. *Advanced Persistent Threat*. [online]. [cit.20.8.2016]. Available from: <https://www.isouvislosti.cz/advanced-persistent-threat>
7. *Advanced Persistent Threats: How They Work*. [online]. [cit.10.7.2016]. Available from: <https://www.symantec.com/theme.jsp?themeid=apt-infographic-1>
8. *Adware*. [online]. [cit.10.8.2016]. Available from: <http://www.mhsaoit.com/computer-networking-previous-assignments/324-lesson-16-h-the-secret-history-of-hacking>
9. *Android Ransomware now targets your Smart TV, Too!* [online]. [cit.14.8.2016]. Available from: <https://thehackernews.com/2016/06/smart-tv-ransomware.html>
10. *Android version market share distribution among smartphone owners as of May 2016*. [online]. [cit.14.8.2016]. Available from: <http://www.statista.com/statistics/271774/share-of-android-platforms-on-mobile-devices-with-android-os/>
11. BALIGA, Arati, Liviu IFTODE and Xiaoxin CHEN. Automated Containment of Rootkits Attacks. *Computers & Security*, 2008, vol. 27, No. 7–8, pp. 323–334.
12. BAUDIŠ, Pavel. Programy typu rootkit. Dalšíhrozba pro Windows. *CHIP*, 2005, No. 7, p. 14
13. *Beware of Fake Android Prisma Apps Running Phishing, Malware Scam* [online]. [cit.14.8.2016]. Available from: <https://www.hackread.com/fake-android-prisma-app-phishing-malware/>
14. *Botnet – Historical List of Botnets*. [online]. [cit.15.8.2016]. Available from: [http://www.liquisearch.com/botnet/historical\\_list\\_of\\_botnets](http://www.liquisearch.com/botnet/historical_list_of_botnets)
15. *Botnet*. [cit.8.7.2016]. Available from: <http://research.omicsgroup.org/index.php/Botnet>
16. *Botnet*. [online]. [cit.15.7.2016]. Available from: <https://en.wikipedia.org/wiki/Botnet>
17. *Botnets*. [online]. [cit.15.7.2016]. Available from:
  
18. *Botnety: nová internetová hrozba*. [online]. [cit.15.7.2016]. Available from: <http://www.lupa.cz/clanky/botnety-internetova-hrozba/>
19. *Bots and Botnets – A growing Threat*. [online]. [cit.11.8.2016]. Available from: <https://us.norton.com/botnet/>
20. *Buffalo Spammer jde na 7 let za mříže kvůli rozesílání nevyžádané pošty*. [online]. [cit.14.8.2016]. Available from: [http://technet.idnes.cz/buffalo-spammer-jde-na-7-let-za-mrize-kvuli-rozesilani-nevyzadane-posty-13i-/tec\\_reportaze.aspx?c=A040528\\_28629\\_tec\\_aktuality](http://technet.idnes.cz/buffalo-spammer-jde-na-7-let-za-mrize-kvuli-rozesilani-nevyzadane-posty-13i-/tec_reportaze.aspx?c=A040528_28629_tec_aktuality)
21. CARL, Glenn, Richard BROOKS and Rai SURESH. Wavelet Based Denial-of-Service Detection. *Computers & Security*, 2006, vol. 25, No. 8, pp. 600–615
22. CHOO, Kim-Kwang Raymond. *Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences* [online]. Canberra: Australian Institute of Criminology, c2009, [cit.19.3.2014]. ISBN 978-1-921532-33-7. Available from: <http://www.aic.gov.au/documents/3/C/1/%7b3C162CF7-94B1-4203-8C57-79F827168DD8%7drpp103.pdf>
23. *Co je to botnet a jak se šíří?* [online]. [cit.15.7.2016]. Available from:

24. Co je to kyberšikana a jak se projevuje? [online]. [cit.19.8.2016]. Available from: <http://www.bezpecne-online.cz/pro-rodice-a-ucitele/teenageri-a-komunikace-na-internetu/co-je-to-kybersikana-a-jak-se-projevuje.html>
25. Čo sa skrýva v prílohe podvodných e-mailov?[online]. [cit.15.8.2016]. Available from: <https://blog.nic.cz/2014/07/23/co-sa-skriva-v-prilohe-podvodnych-e-mailov-2/>
26. Co znamená přípona souboru SCR. [online]. [cit.14.8.2016]. Available from: <http://www.solvusoft.com/cs/file-extensions/file-extension-scr/>
27. Combating Cybercrime in a Digital Age. [online]. [cit.7.5.2016]. Available from: <https://www.europol.europa.eu/ec3>
28. Computer-generated 'Sweetie' catches online predators. [online]. [cit.19.8.2016]. Available from: <http://www.bbc.com/news/uk-24818769>
29. Convicted spammer challenging Va. law[online]. [cit.14.8.2016]. Available from: [http://www.usatoday.com/tech/news/techpolicy/2007-09-12-spammer-va\\_N.htm](http://www.usatoday.com/tech/news/techpolicy/2007-09-12-spammer-va_N.htm)
30. Cyber Terrorism: How Dangerous is the ISIS Cyber Caliphate Threat? [online]. [cit.20.8.2016]. Available from: <http://www.govtech.com/blogs/lohrmann-on-cybersecurity/Cyber-Terrorism-How-Dangerous-is-the-ISIS-Cyber-Caliphate-Threat.html>
31. Cybercrime. [online]. [cit.1.2.2015]. Available from: <http://www.britannica.com/EBchecked/topic/130595/cybercrime/235699/Types-of-cybercrime>
32. Digital Doom's Digi World, 2008. ISSN 1802-047X. [online]. [cit.14.8.2016]. Available from: <http://www.ddworld.cz/software/windows/jak-se-krade-pomoci-internetu-phishing-v-praxi.html>
33. Distribuované výpočty. [online]. [cit.2.11.2013]. Available from: <http://dc.czechnationalteam.cz/>
34. Disturbing ISIS video shows militants beheading four prisoners and gunman executing shoppers at market. [online]. [cit.20.8.2016]. Available from: <http://www.mirror.co.uk/news/world-news/disturbing-isis-video-shows-militants-7306017>
35. DOČEKAL, Daniel. Bruce Schneier: Internet věci přinese útoky, které si neumíme představit. [online]. [cit.10.8.2016]. Available from: <http://www.lupa.cz/clanky/bruce-schneier-internet-veci-prinese-utoky-ktere-si-neumime-predstavit/>
36. DOČEKAL, Daniel. Google: Adware napadá miliony zařízení a poškozuje inzerenty, weby i uživatele. [online]. [cit.10.8.2016]. Available from: <http://www.lupa.cz/clanky/google-adware-napada-miliony-zarizeni-a-poskozuje-inzerenty-weby-i-uzivatele/>
37. Additional Protocol. ETS No. 189 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189>
38. DODGE, Ronald. C., Curtis CARVE and Aaron J. FERGUSON. Phishing for User Security Awareness. *Computers & Security*, 2007, vol. 26, No. 1, pp. 73–80.
39. Dvanáctiletá dívka se zabila po téměř roční šikaně na internetu. [online]. [cit.19.8.2016]. Available from: <https://www.novinky.cz/zahranicni/amerika/313386-dvanactileta-divka-se-zabila-po-temer-rocni-sikane-na-internetu.html>
40. Estonia recovers from massive DDoS attack. [online]. [cit. 4. 3.2010] Available from: [http://www.usatoday.com/tech/news/techpolicy/2007-09-12-spammer-va\\_N.htm](http://www.usatoday.com/tech/news/techpolicy/2007-09-12-spammer-va_N.htm)[http://www.computerworld.com/s/article/9019725/Estonia\\_recovers\\_from\\_massive\\_DDoS\\_attack](http://www.computerworld.com/s/article/9019725/Estonia_recovers_from_massive_DDoS_attack)
41. Exclusive: Computer Virus Hits U.S. Drone Fleet. [online]. [cit.10.7.2016]. Available from: <https://www.wired.com/2011/10/virus-hits-drone-fleet/>
42. Fight against cyber crime: cyber patrols and Internet investigation teams to reinforce the EU strategy. [online]. [cit.10.7.2016]. Available from: <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1827>
43. Flappy Bird Clones Help Mobile Malware Rates Soar. [online]. [cit.14.8.2016]. Available from: <http://www.mcafee.com/us/security-awareness/articles/flappy-bird-clones.aspx>
44. FLocker Mobile Ransomware Crosses to Smart TV. [online]. [cit.14.8.2016]. Available from: <http://blog.trendmicro.com/trendlabs-security-intelligence/flocker-ransomware-crosses-smart-tv/>
45. France drops controversial 'Hadopi law' after spending millions. [online]. [cit.15.7.2016]. Available from: <https://www.theguardian.com/technology/2013/jul/09/france-hadopi-law-anti-piracy> etc.
46. Fridge caught sending spam emails in botnet attack. [online]. [cit.17.5.2016]. Available from: <http://www.cnet.com/news/fridge-caught-sending-spam-emails-in-botnet-attack/>
47. GONZÁLES-TALAVÁN, Guillermo. A Simple, Configurable SMTP Anti-spam Filter: Greylists. *Computers&Security*, 2006, vol. 25, No. 3, pp. 229–236.

48. GOODMAN, Marc. *A vision of crimes in the future*. [online]. [cit.13.11.2014]. Available from: [https://www.ted.com/talks/marc\\_goodman\\_a\\_vision\\_of\\_crimes\\_in\\_the\\_future#t-456071](https://www.ted.com/talks/marc_goodman_a_vision_of_crimes_in_the_future#t-456071)
49. *Google says the best phishing scams have a 45-percent success rate*. [online]. [cit. 14.8.2016]. Available from: <https://www.engadget.com/2014/11/08/google-says-the-best-phishing-scams-have-a-45-percent-success-r/>
50. GREENBERG, Andy. *Hackers remotely kill a Jeep on the highway – with me in it*. [online]. [cit.4.5.2016]. Available from: <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>
51. GRIFFITHS, Mark. Computer Crime and Hacking: a Serious Issue for the Police? *The Police Journal*, 2000, vol. 73, No. 1, pp. 18–24.
52. GRŮVNA, Tomáš and Radim POLČÁK. *Kyberkriminalita a právo*. Prague: Auditorium, 2008
53. *Hackeři se vydávají za Anonymous a hrozí útokem českým firmám*. [online]. [cit.16.8.2015]. Available from: <http://www.lupa.cz/clanky/hackeri-vydavajici-se-za-anonymous-hrozi-utokem-na-ceske-firmy-chteji-zaplatit/>
54. *Hackeři zaútočili na uživatele Facebooku*. [online]. [cit.16.8.2015]. Available from: <http://tech.ihned.cz/c1-37133210-hackeri-zautocili-na-uzivatele-facebooku-chteli-jejich-hesla>
55. HILL, Kashmir. *These two Diablo III players stole virtual armor and gold — and got prosecuted IRL*. [online]. [cit.10.8.2015]. Available from: <http://fusion.net/story/137157/two-diablo-iii-players-now-have-criminal-records-for-stealing-virtual-items-from-other-players/>
56. *Historical list of botnets*. [online]. [cit.15.8.2016]. Available from: <http://jpdias.me/botnet-lab/history/historical-list-of-botnets.html>
57. *Historical Maps of Computer Networks*. [online]. [cit.10.7.2016]. Available from: <https://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/historical.html>
58. HOŘEJŠÍ, Jaromír. *Falešný exekuční příkaz ohrožuje uživatele českých bank*. [online]. [cit.15.8.2016]. Available from: <https://blog.avast.com/cs/2014/07/17/falesny-exekucni-prikaz-ohrozuje-uzivatele-ceskych-bank-2/>
59. *How do APTs work? The Lifecycle of Advanced Persistent Threats (Infographic)*. [online]. [cit. 10. 7. 2016]. Available from: <https://blogs.sophos.com/2014/04/11/how-do-apt-work-the-lifecycle-of-advanced-persistent-threats-infographic/>
60. *How to use Wireshark to capture, Filter and inspect Packets*. [online]. [cit.15.7.2016]. Available from: <http://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/>
61. *Islamic State Hacking Division*. [online]. [cit.20.8.2016]. Available from: [https://ent.siteintelgroup.com/index.php?option=com\\_customproperties&view=search&task=tag&bind\\_to\\_category=content:37&tagId=698&itemId=1355](https://ent.siteintelgroup.com/index.php?option=com_customproperties&view=search&task=tag&bind_to_category=content:37&tagId=698&itemId=1355)
62. *Jessica Logan – The Rest of the Story*. [cit.8.8.2016]. Available from: <http://nobullying.com/jessica-logan/>
63. JIRÁSEK, Petr, Luděk NOVÁK and Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. [online]. 2nd updated edition. Prague: AFCEA, 2015, p. 57 and 73. [online]. [cit.10.7.2016]. Available from: <https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovník-kyberneticke-bezpecnosti---druhe-vydani/>
64. JIROVSKÝ, Václav and Oldřich KRULÍK. Základní definice vztahující se k tématu. *Security magazín*, 2007, vol. 14, No. 2, p. 47.
65. *Judge, 69, who downloaded child porn facing 'catastrophic humiliation'*. [online]. [cit.1.9.2009]. Available from: <http://news.sciencemag.org/social-sciences/2015/02/facebook-will-soon-be-able-id-you-any-photo>
66. *Kevin Mitnick Case: 1999*. [online]. [cit.2.11.2011]. Available from: <http://www.encyclopedia.com/doc/1G2-3498200381.html>
67. KOLOUCH, Jan, Pavel BAŠTA et al. *CyberSecurity*. Prague: CZ.NIC, 2019. ISBN 978-80-88168-31-7.
68. KOLOUCH, Jan. Evolution of Phishing and Business Email Compromise Campaigns in the Czech Republic. In: *Academic and Applied Research in Military and Public Management Science*. Budapest: National University of Public Service, 2018, pp. 83–100. ISSN 2498-5392
69. KOLOUCH, Jan. *CyberCrime*. Prague: CZ.NIC, 2016. ISBN 978-80-88168-15-7
70. KOLOUCH, Jan and Andraera KROPÁČOVÁ. Ransomware. In: ZHUANG, Xiaodong. *Recent Advances in Computer Science: Proceedings of the 19th International Conference on Computers*. B.m.: B.n., 2015, pp. 304–307. Recent Advances in Computer Engineering Series, [Nr. 32]. ISBN 978-1-61804-320-7. ISSN 1790-5109.
71. *Kybergrooming*. [online]. [cit.19.8.2016]. Available from: <http://www.policie.cz/clanek/vite-co-je-kybersikana.aspx>
72. *Kyberšikana I, II*. [online]. [cit.19.8.2016]. Available from: <https://www.e-bezpecci.cz/index.php/component/content/article/7-o-projektu/925-materialy>
73. *Kyberšikana I, II*. [online]. [cit.19.8.2016]. Available from: <https://www.e-bezpecci.cz/index.php/component/content/article/7-o-projektu/925-materialy>
74. LEVY, Steven. *Hackers: Heroes of the Computer Revolution* Sebastopol, CA: O'Reilly Media, pp. 32–41. ISBN 978-1449388393.
75. LI, Tao, GUAN, Zhihong, WU, Xianyong. Modeling and Analyzing the Spread of Active Worms Based on P2P Systems. *Computers & Security*, 2007, vol. 26, No. 3, pp. 213–218.
76. *Malware, mayhem, and the McColo takedown*. [online]. [cit.14.8.2016]. Available from: <http://betanews.com/2008/11/13/malware-mayhem-and-the-mccolo-takedown/>

77. MARCIÁ-FERNANDÉZ, Gabriel, Jesús E. DÍAZ-VERDEJO and Pedro GARCÍA-TEODORO. Evaluation of a Low-rate DoS Attack Against Application Servers. *Computers & Security*, 2008, vol. 27, No. 7–8, pp. 335–354.
78. MATĚJKA, Michal. *Počítačová kriminalita*. Prague: Computer Press, 2002
79. MELOY, Reid J. *STALKING (OBSESSIONAL FOLLOWING): A REVIEW OF SOME PRELIMINARY STUDIES*. [online]. [cit.3.10.2015]. Available from: [http://forensis.org/PDF/published/1996\\_StalkingObsessi.pdf](http://forensis.org/PDF/published/1996_StalkingObsessi.pdf)
80. MINAŘÍK, Pavel. *Wireshark – Paketová analýza pro všechny*. [online]. [cit.18.8.2016]. Available from: <https://www.systemonline.cz/it-security/wireshark-paketova-analyza-pro-vsechny.htm>
81. MITNICK, Kevin D. and William L., SIMON. *Ghost in the Wires: my adventures as the world's most wanted hacker*. New York: Little, Brown & Co, 2012. ISBN 9780316037723.
82. MITNICK, Kevin D. *The art of intrusion: the real stories behind the exploits of hackers, intruders & deceivers*. Indianapolis: Wiley, 2006. ISBN 0-471-78266-1.
83. MUELLER, Robert. [online]. [cit.3.4.2013]. Available from: <https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies>
84. *Největší hackerský útok potvrzen. V ohrožení jsou stovky miliónů uživatelů*. [online]. [cit.16.8.2015]. Available from: <https://www.novinky.cz/internet-a-pc/bezpecnost/405260-nejvetsi-hackersky-utok-potvrzen-v-ohrozeni-jsou-stovky-milionu-uzivatelu.html>
85. *New Ransomware Encrypts Your Game Files*. [online]. [cit.14.8.2016]. Available from: <https://techcrunch.com/2015/03/24/new-ransomware-encrypts-your-game-files/>
86. NIGAM, Ruchna. *A timeline of Mobile Botnets*. [online]. [cit.12.7.2016]. Available from: <https://www.botconf.eu/wp-content/uploads/2014/12/2014-2.2-A-Timeline-of-Mobile-Botnets-PAPER.pdf>
87. OWASP, XSS [online]. [cit.15.7.2016]. Available from: [https://www.owasp.org/index.php/Cross-site\\_Scripting\\_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))
88. *Password Sniffer Spy*. [online]. [cit.18.8.2016]. Available from: <http://securityxploded.com/password-sniffer-spy.php>
89. *Phishing Activity Trends Report*. [online]. [cit.14.8.2016]. Available from: [https://docs.apwg.org/reports/apwg\\_trends\\_report\\_q1\\_2016.pdf](https://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf)
90. *Phishing by the Numbers: Must-Know Phishing Statistics 2016*. [online]. [cit. 14.8.2016]. Available from: <https://blog.barkly.com/phishing-statistics-2016>
91. PLETZER, Valentin. Demaskovaný spyware. *CHIP*, 2007, No. 10, pp. 116–120.
92. PLOHMANN, Daniel, Elmar GERHARDS-PADILLA and Felix LEDER. *Botnets: Detection, Measurement, Disinfection & Defence*. ENISA, 2011. [online]. [cit.17.5.2015], p. 14. Available from: <https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence>
93. *Policejní ransomware*. [online]. [cit.14.8.2016]. Available from: [https://www.f-secure.com/documents/996508/1018028/multiple\\_ransomware\\_warnings.gif/8d4c9ca2-fc77-433d-ac16-7661ace37f88?t=1409279719000](https://www.f-secure.com/documents/996508/1018028/multiple_ransomware_warnings.gif/8d4c9ca2-fc77-433d-ac16-7661ace37f88?t=1409279719000)
94. *Postřehy z bezpečnosti: Ransomware šestkrát jinak*. [online]. [cit.14.8.2016]. Available from: <https://www.root.cz/clanky/postrehy-z-bezpecnosti-ransomware-sestkrat-jinak/>
95. POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Aleš Čeněk, 2005
96. *Pozor na zprávu o údajné neuhrazené pohledávce - jedná se o podvod*. [online]. [cit.15.8.2016]. Available from: <https://www.csirt.cz/page/2073/pozor-na-zpravu-o-udajne-neuhrazene-pohledavce---jedna-se-o-podvod/>
97. *Pozor na zprávu o výzvě k úhradě před exekucí - jedná se o podvod*. [online]. [cit.15.8.2016]. Available from: <https://www.csirt.cz/news/security/?page=87>
98. PROSISE, Chris and Kevin MANDIVA. *Incident Response & Computer Forensic, second edition*. Emeryville: McGraw-Hill, 2003
99. RAK, Roman and Radek KUMMER. Informační hrozby v letech 2007–2017. *Security magazín*, 2007, vol. 14, No. 1, p. 4.
100. *Ransomware*. [online]. [cit.14.8.2016]. Available from: <https://www.trendmicro.com/vinfo/us/security/definition/ransomware>
101. *Riziková komunikace: Kybergrooming* [online]. [cit.19.3.2014]. Available from: <http://www.e-nebezpeci.cz/index.php/rizikova-komunikace/kybergrooming>
102. SCHNEIER, Bruce. *Crime: The Internet's Next Big Thing*. [online]. [cit.6.11.2007]. Available from: <https://www.schneier.com/cryptogram/archives/2002/1215.html>
103. SCHNEIER, Bruce. *The Internet of Things Will Turn Large-Scale Hacks into a Real World Disasters*. [online]. [cit.10.8.2016]. Available from: <https://motherboard.vice.com/read/the-internet-of-things-will-cause-the-first-ever-large-scale-internet-disaster>
104. SCHNEIER, Bruce. *The Seven Types of Hackers*. [online]. [cit.16.8.2015]. Available from: [https://www.schneier.com/blog/archives/2011/02/the\\_seven\\_types.html](https://www.schneier.com/blog/archives/2011/02/the_seven_types.html)
105. SCHRYEN, Guido. The Impact that Placing Email Addresses on the Internet Has on the Receipt of Spam: An Empirical Analysis. *Computers & Security*, 2007, vol. 26, No. 5, pp. 361–372.

106. Selfmite – *Android SMS worm Selfmite returns, more aggressive than ever*. [online]. [cit.14.8.2016]. Available from: <http://www.pcworld.com/article/2824672/android-sms-worm-selfmite-returns-more-aggressive-than-ever.html>
107. Škodlivý kód cílí na mobily, šíří se jako lavina. [online]. [cit.17.5.2016]. Available from: <https://www.novinky.cz/internet-a-pc/bezpecnost/401956-skodlivy-kod-cili-na-mobily-siri-se-jako-lavina.html>
108. Sledování zásilky České pošty aneb nová havěť. [online]. [cit.14.8.2016]. Available from: <http://www.viry.cz/sledovani-zasilky-ceske-posty-aneb-nova-havet/>
109. SMEJKAL, Vladimír, Tomáš SOKOL and Martin VLČEK. *Počítačové právo*. Prague: C. H. Beck, 1995
110. Smejkal, Vladimír. *Kriminalita v prostředí informačních systémů a rekonstrukce trestního zákoníku*. *Trestněprávní revue*, 2003, vol. 2, No. 6, p. 161.
111. Smejkal, Vladimír. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015
112. *Spam Statistics and Facts*. [online]. [cit.14.8.2016]. Available from: <http://www.spamlaws.com/spam-stats.html>
113. *Spam statistics*. [online]. [cit.14.8.2016]. Available from: <https://www.spamcop.net/spamstats.shtml>
114. STRAUS, Jiří et al. *Kriminalistická metodika*. Plzeň: Aleš Čeněk, 2006
115. *Stuxnet*. [online]. [cit.23.7.2016]. Available from: <https://cs.wikipedia.org/wiki/Stuxnet>
116. *Targeted cyberattacks logbook*. [online]. [cit.10.7.2016]. Available from: <https://apt.securelist.com/#secondPage>
117. TAYLOR, Harriet. *How the "Internet of Things" could be fatal*. [online]. [cit.17.6.2016]. Available from: <http://www.cnn.com/2016/03/04/how-the-internet-of-things-could-be-fatal.html>
118. *TCP handshake krok za krokem*. [online]. [cit.18.8.2016]. Available from: <http://www.svetsiti.cz/clanek.asp?cid=TCP-handshake-krok-za-krokem-3122000>
119. *The Internet Organised Crime Threat Assessment (iOCTA) 2014*. [online]. [cit.10.8.2015]. Available from: <https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta>
120. *The Malware Museum @ Internet Archive*. [online]. [cit.17.5.2016]. Available from: <https://labsblog.f-secure.com/2016/02/05/the-malware-museum-internet-archive/>
121. *The testimony of an ex-hacker*. [online]. [cit.26.9.2008]. Available from: <http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/testimony.html>
122. *The very first mobile malware: how Kaspersky Lab discovered Cabir*. [online]. [cit.29.6.2015]. Available from: <http://www.kaspersky.com/about/news/virus/2014/The-very-first-mobile-malware-how-Kaspersky-Lab-discovered-Cabir>
123. Tinba: W32. *Tinba (Tiny banker)*. [online]. [cit.15.8.2016]. Available from: [https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp\\_w32-tinba-tinybanker.pdf](https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_w32-tinba-tinybanker.pdf)
124. *Tip of the month July 2016 – Avoid getting hooked by Phishing*. [online]. [cit.14.8.2016]. Available from: <http://www.intermanager.org/cybersail/tip-of-the-month-july-2016-avoid-getting-hooked-by-phishing/>
125. *Top Spammer Sentenced to Nearly Four Years*. [online]. [cit.14.8.2016]. Available from: <http://www.pcworld.com/article/148780/spam.html>
126. Convention on Cybercrime. <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>
127. *United Nations Manual on the prevention and control of computer-related crime*. [online]. [cit.20.8.2016]. Available from: [http://216.55.97.163/wp-content/themes/bcb/bdf/int\\_regulations/un/CompCrims\\_UN\\_Guide.pdf](http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_UN_Guide.pdf)
128. *Války síťových robotů – jak fungují sítě botnets*. [online]. [cit.15.7.2016]. Available from: [http://tmp.testnet-8.net/docs/h9\\_botnet.pdf](http://tmp.testnet-8.net/docs/h9_botnet.pdf)
129. *Víte co je KYBERŠIKANA?* [online]. [cit.19.8.2016]. Available from: <http://www.policie.cz/clanek/vite-co-je-kybersikana.aspx>
130. *Výzkum rizikového chování českých dětí v prostředí internetu 2014*. [online]. [cit.19.8.2016]. Available from: [https://www.e-bezpeci.cz/index.php/ke-stazeni/doc\\_download/61-vyzkum-rizikoveho-chovani-eskych-dti-v-prostedi-internetu-2014-prezentace](https://www.e-bezpeci.cz/index.php/ke-stazeni/doc_download/61-vyzkum-rizikoveho-chovani-eskych-dti-v-prostedi-internetu-2014-prezentace)
131. *Warning! Over 900 Million Android Phones Vulnerable to New „QuadRooter“ Attack*. [online]. [cit.10.8.2016]. Available from: <https://thehackernews.com/2016/08/hack-android-phone.html>
132. *WATCH: ISIS Downs Prisoners Alive & Blows Hostages Up With RPG & Kills Others With Explosives – Graphic video*. [online]. [cit.20.8.2016]. Available from: <https://www.zerocensorship.com/uncensored/isis/drowns-prisoners-alive-blows-hostages-up-with-rpg-kills-others-with-explosives-graphic-video-132382>
133. **WILSON Tracy, V.** *How Phishing Works*. [online]. [cit.14.8.2016]. Available from: <http://computer.howstuffworks.com/phishing.htm>
134. Xshqi – *Android Worm on Chinese Valentine's day*. [online]. [cit.14.8.2016]. Available from: <https://securelist.com/blog/virus-watch/65459/android-worm-on-chinese-valentines-day/>
135. *Yahoo řeší, jestli má hacker opravdu údaje o 200 milionech účtů*. [online]. [cit.16.8.2015]. Available from: <http://www.lupa.cz/clanky/yahoo-resi-jestli-hacker-opravdu-ma-udaje-o-200-milionech-tamnich-uctu/>



136. YAR, Majid. Computer Hacking: Just Another Case of Juvenile Delinquency? *The Howard Journal*, 2005, vol. 44, No. 4, pp. 387–399.
137. ZETTER, Kim. *Is It Possible for Passengers to Hack Commercial Aircraft?* [online]. [cit.5.5.2016]. Available from: <https://www.wired.com/2015/05/possible-passengers-hack-commercial-aircraft/>
138. *Znovu se objevily podvodné zprávy.* [online]. [cit.15.8.2016]. Available from: <https://www.csirt.cz/news/security/?page=97>