AARMS Vol. 17, No. 3 (2018) 83–100. **10.32565/aarms.2018.3.6**

Evolution of Phishing and Business Email Compromise Campaigns in the Czech Republic

Jan KOLOUCH[1]

Cyberspace is an environment in which cyber-attacks can be committed. Fraudulent attacks are one of the oldest cyber-attacks of all. The aim of this article is to familiarize the reader with the evolution of phishing and Business Email Compromise (BEC) attacks that occurred to a large extent in the cyberspace of the Czech Republic from 2014 to 2018. The article describes scam, phishing and BEC definitions, as well as individual ways of implementing specific attacks. Special attention is also paid to the possible criminal liability of the attacker for the described cyber-attacks, both according to the international legal regulations (enshrined in the Convention on Cybercrime) and according to the legislation of the Czech Republic.

Keywords: *scam, phishing, Business Email Compromise, cybercrime, cyber-attack, fake email, execution*

Introduction

Cybercrime[2] is considered a new kind of crime but the major part of this criminal offence uses or transfers notorious kinds of illegal conduct (e.g. fraud, copyright breach, theft, bullying, etc.) in the digital environment where such crimes can be committed in a more "effective" way compared to the real world.

The approach which is very frequently adopted by attackers in a virtual environment can be compared to an "area bombing" while with such massive extent of the attack, one can assume that there will be someone who will fall for it.

On the other hand, currently there are more and more cyber-attacks[3] which are very specifically targeted, prepared for a long time and which use elements of social engineering in a way that the attackers can achieve their goal.

[1] Associate professor, dr. jur., Ph.D., Ambis (www.ambis.cz/); e-mail: jan.kolouch@ambis.cz

[2] Cybercrime represents a crime where the means of information and communication technologies are used as a tool for committing a crime and also represent a target for the perpetrator's attack, while such an attack is a criminal offence. All this is subject to the condition that the means are used or misused in the information, system, program or communication environment (i.e. in cyberspace). See [12: 55].

[3] Prosise and Mandiva define a "computer security incident" (that can be perceived as a cyber-attack or cyber-crime) as an unlawful, illegal, unauthorised, unacceptable action that concerns a computer system or a computer network. Such action can take the form of, for instance personal data theft, spam or other intrusion, misappropriation, proliferation or possession of child pornography and others. [16: 13] The other definition can be found in [5: 9; 12: 55]. Cyber-attack can also be defined as any illegal action by the offender in the cyberspace, targeted against the interests of another person. Such action needs not always constitute a criminal offence; the key is that it hinders the everyday life of the injured. A cyber-attack can be either completed or it can be in preparation or only attempted.

This paper primarily deals with the evolution of fraudulent attacks in the Czech Republic. However, in order to understand the issue better, it provides definitions of the terms “scam”, “phishing” and “Business Email Compromise” first (as well as the specifics of such cyber-attacks) and presents some significant fraudulent attacks that occurred in the Czech Republic. Towards the end, the paper deals with the possibilities of criminal prosecution of the perpetrator for such acts.

Cyber Attacks: Scam, Phishing, Business Email Compromise (BEC)

Scam

The term “scam” is simply defined as: *a* dishonest scheme; a fraud. [18] However, from the point of view of cybercrime, such a definition is insufficient and it would include a much wider group of criminal acts, not just cybercrime.

A more suitable definition of scam, from the point of view of cybercrime, can be found in the Business Dictionary: “A fraudulent scheme performed by a dishonest individual, group, or company in an attempt to obtain money or something else of value. Scams traditionally resided in confidence tricks, where an individual would misrepresent themselves as someone with skill or authority, i.e. a doctor, lawyer, investor. After the internet became widely used, new forms of scams emerged such as lottery scams, scam baiting, email spoofing, phishing, or request for helps. These are considered to be email fraud. Also see phishing, scheme.” [17]

Scam represents spam[4] with criminal or other deceptive contents, while scam currently constitutes a significant part of spam and its purpose is, typically with the use of social engineering, to gain the user’s trust and make the user carry out the required tasks (e.g. open an email attachment, go to a certain URL, etc.). Scam may include *phishing, malware, 419, hoax, fake lotteries and offers, donor scam, cold-call scam, Facebook-like scam etc.*[5]

From the point of view of general taxonomy, the term “scam” is a broader term than the terms “phishing” and “Business Email Compromise”. It is also possible to say that scam represents a distribution platform which is used by cyber attackers, usually in connection with social-engineering techniques.

[4] Spam means any unsolicited message. Very often, this term is incorrectly connected with unsolicited business messages only.

[5] Phishing—see below. 419 scam—this refers to a fraud scheme also known as the Nigerian Prince scam. Hoax—refers to “chain emails”. Donor scam typically involves requests for help with alleged illness (of a child, family member, etc.) or financial problems. Cold-call scam—this is usually an email from an IT department or company. The message includes information that the user’s computer system has been infected with malware and therefore it is necessary to remotely connect the computer to the IT department to deal with the problem. For further details see e.g. [7].

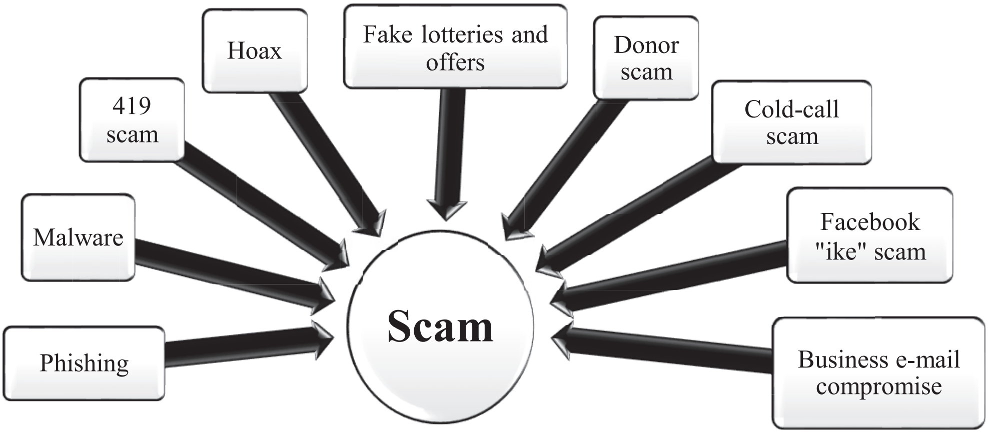
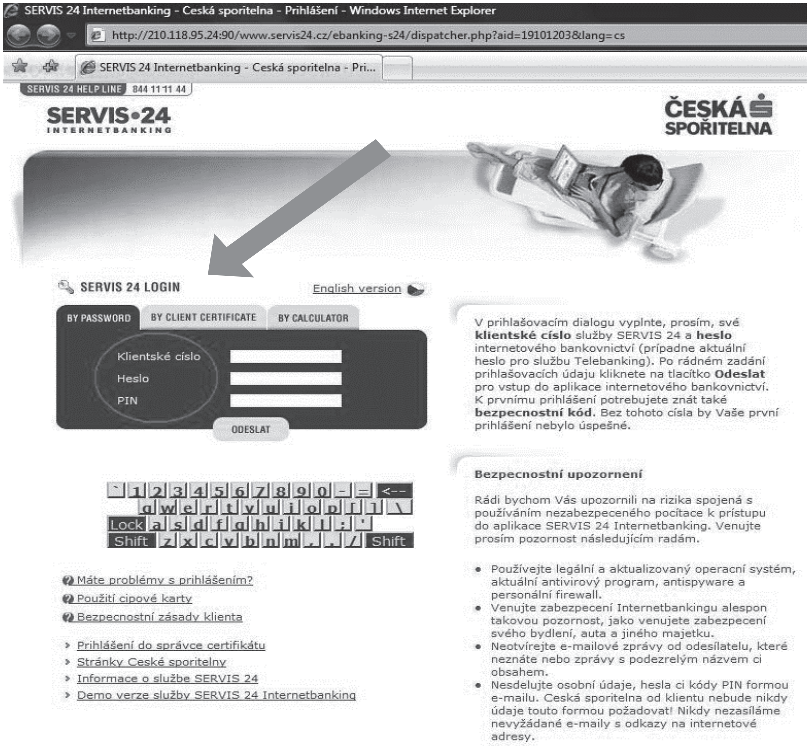


Figure 1. *Scam attacks.* [12: 236]

Phishing

The term "phishing" most frequently refers to a fraudulent or deceptive act the purpose of which is to obtain information about the user, typically the user's name, password, credit card number, PIN, or other data and information which might be used by the attacker.

The principle of a typical phishing attack usually consists in the practice of sending a phishing email to the injured party while at first sight such an email does not arouse suspicion of a fraudulent message. Such email usually contains a link and the user is encouraged to click on it. When the user clicks on the link, it opens a website created by the fraudster. A fraudulent website may imitate any possible website where the user is used to fill in their "login data" or other sensitive information. This usually regards internet banking websites, e-shops, mail servers, social networks, etc.



SERVIS 24 Internetbanking - Ceská sporitelna - Prihlášení - Windows Internet Explorer

http://210.118.95.24:90/www.servis24.cz/ebanking-s24/dispatcher.php?aid=19101203&lang=cs

SERVIS 24 Internetbanking - Ceská sporitelna - Pri...

SERVIS 24 HELP LINE 844 11 11 44

SERVIS 24 LOGIN

Klientské císlo

Heslo

PIN

V prihlašovacím dialogu vyplnte, prosím, své **klientské císlo** služby SERVIS 24 a **heslo** internetového bankovnictví (prípadne aktuální heslo pro službu Telebanking). Po rádném zadání prihlašovacích údaju kliknete na tlacítko **Odeslat** pro vstup do aplikace internetového bankovnictví. K prvnímu prihlášení potrebujete znát také **bezpecnostní kód**. Bez tohoto císla by Vaše první prihlášení nebylo úspešné.

Bezpecnostní upozornení

Rádi bychom Vás upozornili na rizika spojená s používáním nezabezpeceného pocítace k prístupu do aplikace SERVIS 24 Internetbanking. Venujte prosím pozornost následujícím radám.

- Používejte legální a aktualizovaný operacní systém, aktuální antivirový program, antispyware a personální firewall.
- Venujte zabezpecení Internetbankingu alespon takovou pozornost, jako venujete zabezpecení svého bydlení, auta a jiného majetku.
- Neotvírejte e-mailové zprávy od odesílatelu, které neznáte nebo zprávy s podezrelým názvem ci obsahem.
- Nesdelujte osobní údaje, hesla ci kódy PIN formou e-mailu. Ceská sporitelna od klientu nebude nikdy údaje touto formou požadovat! Nikdy nezasíláme nevyžádané e-maily s odkazy na internetové adresy.

SERVIS•24
INTERNETBANKING
ČESKÁ SPOŘITELNA
English version
BY PASSWORD
BY CLIENT CERTIFICATE
BY CALCULATOR
ODESLAT
` 1 2 3 4 5 6 7 8 9 0 - = <--
q w e r t y u i o p [ ] \
Lock a s d f g h j k l ; '
Shift z x c v b n m , . / Shift
Máte problémy s prihlášením?
Použití cipové karty
Bezpecnostní zásady klienta
Prihlášení do správce certifikátu
Stránky Ceské sporitelny
Informace o službe SERVIS 24
Demo verze služby SERVIS 24 Internetbanking

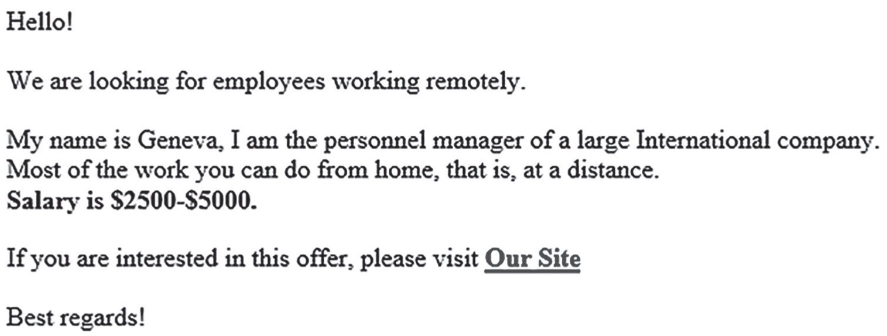
Figure 2. *Phishing site requesting the user to fill in their login data, including the PIN number (2009 attack).* [Print screen created by the author.]

This method of coaxing login data and other sensitive information out of the victim is currently on the decline and only rarely used by attackers. The above act can be called phishing “in a strict sense”.

In the broader sense of the term phishing may refer to any fraudulent act the purpose of which is to inspire confidence, make the user drop their guard, or in any other way make the user accept the scenario prepared by the attacker in advance. In this concept, the user is not requested to fill in the login data but they receive a message (or the user is redirected to a website) which usually contains malware that is able to collect the data itself. This broader concept of phishing may also include e.g. scam[6] etc.

An example of this approach includes, but is not limited to, scam that offers interesting job positions. An example of such emails is shown in Figure 3. Figure 4 shows an analysis of the URL referred to in the email.

[6] In 2014, for example, Google stated that scam, having the character of high-quality phishing, has a 45% success rate if user data are obtained. See e.g. [3].



Hello!

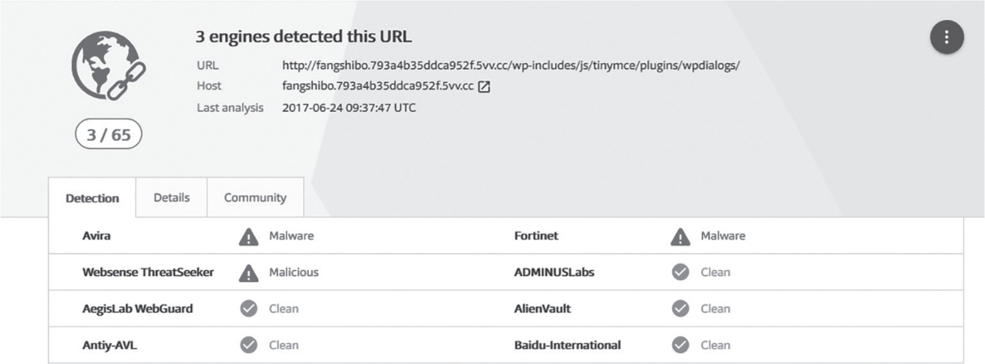
We are looking for employees working remotely.

My name is Geneva, I am the personnel manager of a large International company.
Most of the work you can do from home, that is, at a distance.
Salary is $2500-$5000.

If you are interested in this offer, please visit **Our Site**

Best regards!

Figure 3. *Job offer (attack carried out between 2016 and 2018).*
[Print screen created by the author.]



3 engines detected this URL

URL http://fangshibo.793a4b35ddca952f.5vv.cc/wp-includes/js/tinymce/plugins/wpdialogs/
Host fangshibo.793a4b35ddca952f.5vv.cc
Last analysis 2017-06-24 09:37:47 UTC

Avira	Malware	Fortinet	Malware
Websense ThreatSeeker	Malicious	ADMINUSLabs	Clean
AegisLab WebGuard	Clean	AlienVault	Clean
Antiy-AVL	Clean	Baidu-International	Clean

Figure 4. *Analysis result (attack carried out between 2016 and 2018).*
[Conducted with the tool www.virustotal.com edited by the author.]

The aim of a phishing attack, whether in the narrower or broader sense of the term, is to deceive the user. The difference between the individual forms of the attack consists mainly in the level of cooperation required from the user.

For a phishing attack to be successful, the attacker needs to make use of all social-engineering techniques, while phishing is not focused on emails only. Phishing can be found in instant messages, on social networks, in SMS and MMS messages, chat rooms, scam, false browser applications, etc.

The next step in the evolution of phishing was the implementation of various types of malware directly in the scam message body. To demonstrate the evolution of a phishing attack, I am going to present two important campaigns which took place, or which are taking place, in the Czech Republic. The reason for choosing the two specific attacks is the distinctly innovative approach of the attackers and the link between the technical attack and social engineering.

Case 1 – Debt/Bank/Execution

This phishing campaign hit the Czech Republic to a great extent in 2014 and lasted at least till the end of 2015.[7] The principle of this attack was employed again, with minor modifications, at the end of 2017 and in the first quarter of 2018. The attack itself was prepared with precision and included both phishing and malware distribution (to computer and mobile devices). The entire attack can be divided into the following phases:

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

Ad 1. Phishing campaign

The first prerequisite for the attackers to successfully obtain the funds is an extensive phishing campaign which would trigger a response from a sufficiently large number of persons. In 2014–2015, fraudulent emails were sent out in three consecutive massive waves of phishing messages:

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

The fourth wave of the attack uses what is now a well-established and tried and tested modus operandi, as well as any infected computer system from the previous three waves.

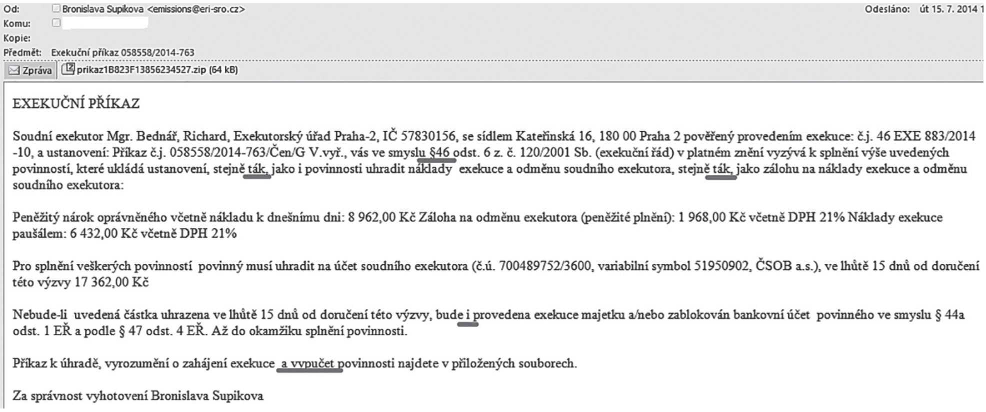
IV. Distress (e.g. podatelna@exekutor.cite etc.); October 2017–March 2018

During the individual campaigns, the "quality (credibility)" of the emails increased and social engineering was used more effectively in relation to the expected victims within the targeted area, i.e. the Czech Republic. However, all of the aforementioned phishing campaigns had at least two characteristics in common. Firstly, the attachment of the email always included a file which looked like a text document but it was an executable file, namely malware: Trojan.[8] The other characteristic in common was the fact that social engineering benefited from concerns of those addressed over lawsuits resulting from a non-existent debt, or distress in the last case.

The first wave of phishing attacks used very poor Czech and the messages were sent from various domains registered in the Czech Republic which were not exactly credible. It used names of various people and existing telephone numbers which could be looked up on the Internet (while the owner of the number had nothing to do with the attack). In the second wave, the Czech language improved. When such phishing attacks started to appear, various

[7] For further information see [14].
[8] For further information see the results from [26].

security organizations and Computer Security Incident Response Team (CSIRT) teams,[9] as well as mass media, issued warnings and provided manuals showing what to do with such messages. [1] [2] [8] [9] [24] Both campaigns were relatively successful but most success was achieved during the third wave when the attacker impersonated a bailiff.



Od: □ Bronislava Supikova <emissions@eri-sro.cz> Odesláno: út 15. 7. 2014 1
Komu: □ [redacted]
Kopie:
Předmět: Exekuční příkaz 058558/2014-763

EXEKUČNÍ PŘÍKAZ

Soudní exekutor Mgr. Bednář, Richard, Exekutorský úřad Praha-2, IČ 57830156, se sídlem Kateřinská 16, 180 00 Praha 2 pověřený provedením exekuce: č.j. 46 EXE 883/2014 -10, a ustanovení: Příkaz č.j. 058558/2014-763/Čen/G V.vyř., vás ve smyslu §46 odst. 6 z. č. 120/2001 Sb. (exekuční řád) v platném znění vyzývá k splnění výše uvedených povinností, které ukládá ustanovení, stejně ták, jako i povinnosti uhradit náklady exekuce a odměnu soudního exekutora, stejně ták, jako zálohu na náklady exekuce a odměnu soudního exekutora:

Peněžitý nárok oprávněného včetně nákladu k dnešnímu dni: 8 962,00 Kč Záloha na odměnu exekutora (peněžité plnění): 1 968,00 Kč včetně DPH 21% Náklady exekuce paušálem: 6 432,00 Kč včetně DPH 21%

Pro splnění veškerých povinností povinný musí uhradit na účet soudního exekutora (č.ú. 700489752/3600, variabilní symbol 51950902, ČSOB a.s.), ve lhůtě 15 dnů od doručení této výzvy 17 362,00 Kč

Nebude-li uvedená částka uhrazena ve lhůtě 15 dnů od doručení této výzvy, bude i provedena exekuce majetku a/nebo zablokován bankovní účet povinného ve smyslu § 44a odst. 1 EŘ a podle § 47 odst. 4 EŘ. Až do okamžiku splnění povinnosti.

Příkaz k úhradě, vyrozumění o zahájení exekuce a vypučet povinnosti najdete v přiložených souborech.

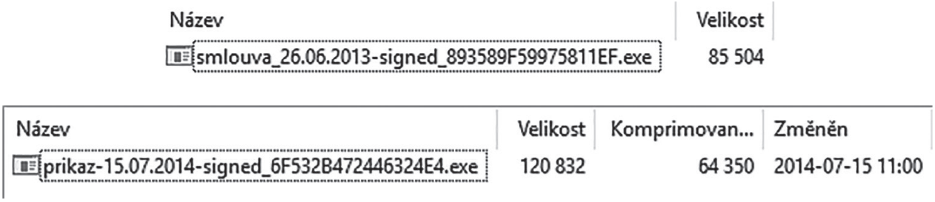
Za správnost vyhotovení Bronislava Supikova

Figure 5. *Fraudulent email sent during the "Distress" wave.*
[Print screen created by the author.]

The text in the Czech language used in the "distress warrant" showed errors, especially in diacritics and contained several overcomplicated sentences. However, it mentioned names of real bailiffs which could be looked up on the Internet (again, the bailiff had nothing to do with the attack) and distress proceedings numbers that looked real.

Ad 2. Installation of malware on the computer

As mentioned above, all phishing campaigns contained the following malware in the email attachment: TrojanDownloader (i.e. malware designed for downloading another malware). The malware was primarily created for and aimed at the Windows XP operating system, the support of which ended in March 2014.



Název	Velikost
smlouva_26.06.2013-signed_893589F59975811EF.exe	85 504

Název	Velikost	Komprimovan...	Změněn
prikaz-15.07.2014-signed_6F532B472446324E4.exe	120 832	64 350	2014-07-15 11:00

Figure 6. *Executable file (malware) contained an attachment to fraudulent emails.*
[Print screen created by the author.]

[9] For more information see e.g. [27].

When the attachment was run, it initiated installation of the "Tinba" malware (bank Trojan horse) which was downloaded from the Internet in the background, while a contract or a distress warrant was shown to the user in a text editor.[10]

Malware was written in the following directory: Users/*user*/AppData/Roaming/brothel. In this directory, ate.exe could be found, which is a file that was created when the executable file from the phishing email was opened. At the same time, a key was created in the registers at HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRun.

Ad 3. Access to online banking

Once the malware had been installed, the attacker waited until the victim logged into their online banking. The malware on the computer was able to detect the communication between the user and the online banking system and the attacker could monitor the communication. The user had almost no chance to recognize the attack as the URL address in the browser belonged to the bank and the communication was secured (HTTPS).

"The theft of sensitive data occurs when a malicious code is input on the bank's official website. Configuration scripts are downloaded from C&C servers (machines which belong to the attackers and are used to control the botnet) and deciphered as mentioned above. The interesting thing is the use of the same format of the configuration files known as Carberp and Spyeye bank Trojans. For each botuid (unique value which identifies the user's environment), a list of user names and passwords is stored on the C&C server. Other scripts are downloaded depending on the bank, i.e. hXXps://andry-shop.com/gate/get_html.js;hXXps://andry-shop.com/csob/gate/get_html.js; or hXXps://yourfashionstore.net/panel/a5kGcvBqtV, and the download occurs if the victim goes to the websites of Česká spořitelna, ČSOB, or Fia." [10]

Ad 4. Installation of malware on a mobile device

The next step of the attacker was to persuade the user that it was necessary to enhance the security when accessing online banking. The victim was offered a website with a choice of the operating system for the mobile device (OS Android, Windows Phone, Blackberry and iPhone), but only the OS Android version allowed the malware to be downloaded to the phone. Attackers used various methods of how to distribute the malware to the phone—from simply sending a text message with a link where the user was supposed to download the programme, to sending a text message and the QR code.

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

The aim of the malware was to get access to and full control over the secondary authentication tool (two-factor authentication) which is, in a majority of cases, represented by a mobile phone. If the user has an operating system other than Android, the following message was displayed: "Please try again later."

[10] For further information see the analysis of Tinba malware operation. [21]

Ad 5. Transfer and siphoning of funds

The last step of the attacker was to siphon off funds from the account of the person attacked and transfer them to an account of a money mule who was supposed to withdraw cash, or transfer it to other accounts. Thanks to the full control (by means of the malware) both over access data for the internet banking (see the computer attacked) and over the secondary authentication tool (see the mobile phone attacked—when the authentication messages were forwarded to the attacker and not displayed to the victim), the attacker could enter a "legitimate" command to transfer the money.

A modification of the last step can be seen in attacks that occurred between 2017 and 2018 when the attackers not always tried to transfer funds to the attacker's bank account but rather requested a transfer of a sum owed with a virtual currency, etc.

Case 2 – Christmas

Further evolution of phishing attacks can be seen during December 2014 (particularly during the Christmas period), in January 2015 and then again in the same period in 2017. The common denominator of the attacks was the type of file stored in the phishing email attachment. In the attacks, users were sent email messages wishing them merry Christmas through an e-card, or they were sent messages with a confirmation of an order for allegedly purchased electronics.

All the attacks had one element in common and that was the malware contained in the email attachment. The malware was a Trojan horse (the most frequently used malware was Kryptik) which was presented as a screen saver. Same as in Case 1, the malware was compressed in a .zip file so as to pass antimalware protection of the given email service. Nevertheless, when the .zip file was unpacked, many users did not consider the *.scr*[11] file to be a defective and executable (*.exe*) program and thus their computer was infected.

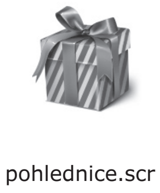
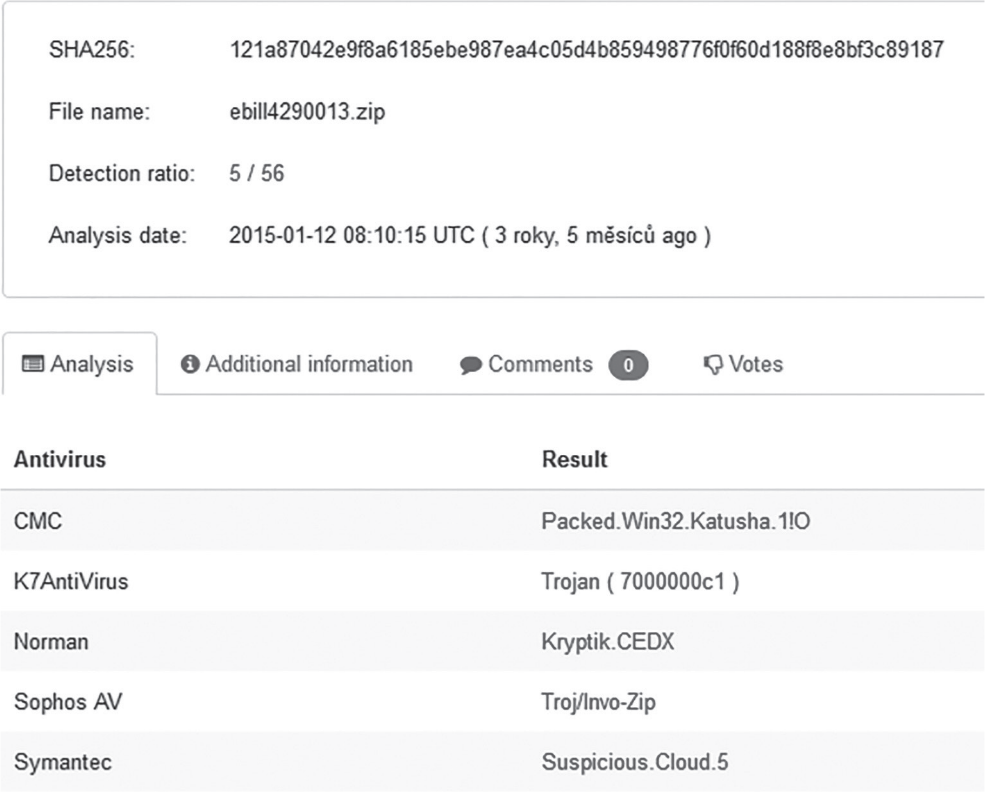


Figure 7. *"Christmas card" attachment – .scr card.*
[Print screen created by the author.]

[11] SCR files are executable files. Primarily they are assigned to the Unknown Apple II File program (found on Golden Orchard Apple II CD Rom). Furthermore, they are also assigned to 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 and FileViewPro. [22]

The attack was specific for several reasons. One reason was the type of file which many users consider to be safe and the other was the timing of the attack. Thanks to various chain emails, users are used to opening e-cards, or attachments that look like e-cards, without careful examination of the contents. Further attacks were planned so that the user had to check whether they really had not ordered some goods which were not delivered to the user due to Christmas holidays.

The last key factor which facilitated the massive extent of this phishing campaign and effective infection of computers with this malware was the relatively long zero-day vulnerability, [25] as the timing of the attack fell on Christmas and Christmas holiday when a number of people (also in anti-virus companies) are off. In the first fortnight of the attack, only a few anti-virus companies were able to analyse that the *pohlednice.scr* file contains malware. (See Figure 7.)



SHA256: 121a87042e9f8a6185ebe987ea4c05d4b859498776f0f60d188f8e8bf3c89187

File name: ebill4290013.zip

Detection ratio: 5 / 56

Analysis date: 2015-01-12 08:10:15 UTC (3 roky, 5 měsíců ago)

Antivirus	Result
CMC	Packed.Win32.Katusha.1!O
K7AntiVirus	Trojan (7000000c1)
Norman	Kryptik.CEDX
Sophos AV	Troj/Invo-Zip
Symantec	Suspicious.Cloud.5

Figure 8. *Result of the analysis 14 days after the attack.*
[Conducted with the tool edited by the author.]

Business Email Compromise (BEC)

Business Email Compromise[12] 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 the FBI, 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 email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds. [4]

Unlike a traditional phishing attack, BEC is targeted at a certain individual or organization. In case of a 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 organization's employees from social networks, 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. [23]

The victims of the BEC scam range from small businesses to large corporations. 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 have 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.

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*[13]
   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 email or telephone. An email attack has typically a spoofed email source code (header) and subject of the request, so it appears very similar to a legitimate request.

[12] BEC scams are also known as "CEO fraud" or "Man-in-the-Email" scams.

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

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 data to his account. 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 targets.)
2. *Preparation of a spoofed email* (to create a spoofed email, publicly available free services are used very often, e.g. 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 € 4,000.)
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, it 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*

Towards the end of this paper on phishing and BEC attacks, I am going to mention some statistics of the Czech national CSIRT team and of the Czech Police, focused on fraudulent acts or spam.

Table 1. *Statistics of CSIRT.cz.*

	2008	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**sum**
Phishing	65	220	209	144	159	175	368	367	363	409	231	2,710
Spam	47	28	103	26	43	73	159	108	290	121	73	1,071
Pharming							18	3	2	3	3	29

Table 2. *Statistics of the Police of the Czech Republic.* [19]

Structure of criminal offences	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**
Fraudulent acts	917	1.303	1.863	2.478	2.932	3.235	3.036
Total share	61.05%	59.36%	59.94%	56.99%	58.37%	60.54%	55.76%

Legal aspects of Phishing and Business Email Compromise (BEC) campaigns

Based on the attacks described above, it is possible to apply the individual provisions of *Convention No. 185 on Cybercrime of 23rd November 2001* to penalize the perpetrator, with necessary modifications according to national legal regulations.

When determining which section of the Convention on Cybercrime is to be applied, it is essential to analyse the attacker's specific acts, particularly the fact whether it is just a fraudulent act or a combined attack, which uses e.g. malware, the aim of which is to identify a specific computer system and only then obtain data in the form of access information.

From this point of view, it is necessary to distinguish the following situations:

1. *Sending a phishing or BEC message, infected file, or a link to an infected website*

Most frequently, the victim is sent an email which contains a link which the user is prompted to follow. Once the user has clicked on the attached link, they are directed to a website, the layout and functions of which do not differ from the authentic website. The phishing website collects data entered on the fake websites and sends them automatically to the offender.

Enclosing the malicious code directly in the email is another way to infect the victim's computer.

From the legal point of view, the *Convention on Cybercrime* classifies the action by the offender, i.e. sending of the file through which the offender may gain control over somebody else's computer, or re-directing to the website containing malware, as an *attempt* or *aiding* or *abetting* to criminal offences. In this case, the action most likely constitutes an attempt to commit a criminal offence as defined in Articles 4 through 6 of the Convention on Cybercrime. For future reference, the above-mentioned articles of the Convention on Cybercrime are described below in detail:

Article 4 of the Convention – Data interference

1. *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.*
2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

   In conjunction with the relevant provisions of national criminal law, this article provides for sanctioning actions consisting of *intentional installation of malware into a computer system without the consent of the system's rightful user.*

Article 5 of the Convention – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

While Article 4 of the Convention defines the merits of a criminal offence against data in a computer system, i.e. the interference with the data does not necessarily cause damage to the computer system (e.g. changing data in a database), this Article protects the functioning of a computer system as a whole, and the actions described in Article 4 here hinder the functioning of the computer system affected.

Article 6 of the Convention – Misuse of devices

1. *Each Party shall adopt such legislative and other measures as may be necessary to establish criminal offences under its domestic law, when committed intentionally and without right:*
   a) *the production, sale, procurement for use, import, distribution or otherwise making available of:*
      i. *a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;*
      ii. *a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,*
      with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and
   b) *the possession of an item referred to in paragraphs a) i. or ii. above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.*

In accordance with the above provision, *all offenders who proliferate,* sell, procure for themselves or others, import, distribute or otherwise make available for instance malware (programmes such as computer worms, Trojan horses, key loggers, etc.) should be sanctioned.

2. *Entering the malicious code in the computer*

From the legal point of view, the action by the offender consisting of the malware installation (without the consent of the rightful user) into the compromised device constitutes a completed criminal offence as defined in Articles 2, 4 and 5 of the Convention on Cybercrime. Article 2 of the Convention defines *"Illegal access"* as committed by a person through gaining an unauthorised access to a computer system or its parts.

From the legal point of view, ***Article 8 of the Convention on Cybercrime—Computer-related fraud—can also be applied to the above described action.***

Each Party shall adopt such legislative and other measures as may be necessary to establish criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a) *any input, alteration, deletion or suppression of computer data,*

b) *any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.*

The above described action, which according to this Article should be criminally punishable, occurs most frequently in conjunction with other actions that the Convention aims to mitigate. For instance, the attacker first obtains the programme that enables him to interfere with a computer system without authorisation (Article 6). Next, he uses the programme obtained to execute the attack by simulating the person's authorisation to dispose with a bank account (Articles 4 and 7). Finally, he may give instructions to transfer money to his benefit or to the benefit of a third party (Article 8).

It is precisely the provisions of Article 8 of the Cybercrime Convention that have been adopted to combat attacks in the form of fraud (typically scam, phishing, pharming, spear phishing, BEC).

According to the Czech criminal law, any conduct having the character of "classic phishing" can be penalized according to *sec. 209* (Fraud) of the Criminal Code, [28] while fraud is completed by self-enrichment. Creation of a website replica and obtaining of login names and passwords could be classified as a preparation of a criminal act, or as an attempt to commit a criminal act, according to sec. 209 of the Criminal Code. Obtaining of access data, including account numbers, payment card numbers and PIN codes, without further use thereof, is not necessarily punishable.

In case of combined forms of phishing attacks, when malware is used to infect the computer, such conduct carried out by the perpetrator needs to be penalized also according to *sec. 230* (unauthorized access to a computer system and data medium) of the Criminal Code. If the purpose of a phishing attack is to gain unauthorized benefit for oneself or others, provisions of *sec. 230, par. 3* of the Criminal Code, may also be applied.

In specific cases, provisions of *sec. 234* of the Criminal Code could also be applied (unauthorized obtaining, forging and modification of a payment means).

Conclusion

As mentioned at the beginning of the paper, fraudulent attacks represent one of the oldest cyber-attacks in general, but especially due to irresponsible and careless behaviour of users, they will be one of the most common types of cyber-attacks in the future.

It is extremely difficult to determine how many fraudulent attacks are carried out all over the world every day. Likewise, it is hard to determine how many clients of the companies attacked reply to a scam, phishing or other defective email. The return rate is estimated at approx. 0.01 and 0.1%.[14] [13: 35]

Although the scam return rate is negligible, with the extent at which emails having the character of scam or phishing are sent, the aforementioned percentage represents a significant financial profit for the perpetrators of the attacks.

2007 prognoses estimated that there were going to be more "typical" phishing scams or campaigns in the future.[15] The prognoses have partly come true as "typical" phishing campaigns are on the decrease, but phishing in the broader sense of the word is booming[16]—new phishing modifications appear and phishing is also connected with other types of attacks (malware, connection to the botnet network, etc.).

References

[1] *Beware of a message about an alleged unpaid claim – it is a scam.* CSIRT.cz (online). www.csirt.cz/page/2073/pozor-na-zpravu-o-udajne-neuhrazene-pohledavce---jedna-se-o-podvod/ (Downloaded: 15.08.2016)

[2] *Beware of a notice to pay before distrain – it is scam.* CSIRT.cz (online). www.csirt.cz/news/security/?page=87 (Downloaded: 15.8.2016)

[3] SOUZA, R. D.: *Beware of Fake Android Prisma Apps Running Phishing, Malware Scam.* HackRead (online), 2016. www.hackread.com/fake-android-prisma-app-phishing-malware/ (Downloaded: 14.08.2016)

[4] FBI: *Business E-mail Compromise: The 3.1 Billion Dollar Scam*. FBI Field Office (online), June 14, 2016. www.ic3.gov/media/2016/160614.aspx (Downloaded: 12.06.2018)

[5] CASEY, E.: *Digital Evidence and Computer Crime: Forensic Science. Computers, and the Internet.* Second Edition. London: Academic Press, 2004.

[6] DODGE, R. C., CARVE, C. A., FERGUSON, J.: Phishing for User Security Awareness. *Computers & Security,* 26 1 (2007), 73–80. DOI: https://doi.org/10.1016/j.cose.2006.10.009

[14] As regards the issue of phishing compare e.g. [20] and [11: 9].

[15] For phishing trends, compare e.g. [6].

[16] According to the following study, phishing has increased by 250% over the last 6 months. See [15].

[7] *Does Microsoft call about computer being infected with virus?* Computer Hope (online), updated: May 21, 2018. www.computerhope.com/issues/ch001385.htm (Downloaded: 14.08.2016)

[8] *Fraudulent emails are back again.* CSIRT.cz (online). www.csirt.cz/news/security/?page=97 (Downloaded: 15.08.2016)

[9] *PODVODNÉ EMAILY hrozí exekucí, nic neplaťte a neotvírejte! (FRAUDULENT EMAILS threaten with a distress warrant—do not pay anything and do not open them!)* TN.cz (online). http://tn.nova.cz/clanek/zpravy/cernakronika/podvodne-emaily-hrozi-exekuci-nic-jim-neplatte-a-neotvirejte.html (Downloaded: 15.08.2016)

[10] HOŘEJŠÍ, J.: *Falešný exekuční příkaz ohrožuje uživatele českých bank. (A false distress warrant puts users of Czech banks at risk.)* avastblog (online), July 17, 2014. https://blog.avast.com/cs/2014/07/17/falesny-exekucni-prikaz-ohrozuje-uzivatele-ceskych-bank-2/ (Downloaded: 15.08.2016)

[11] KOLOUCH, J., VOLEVECKÝ, P.: Criminal law aspects of a phishing attack. *Criminal Law,* 12 (2008), 5–12.

[12] KOLOUCH, J.: *CyberCrime.* Prague: CZ.NIC, 2016.

[13] LANCE, J.: *Phishing without mysteries*. Prague: Grada, 2007.

[14] *Uhraďte dluhy, toto je exekuční příkaz. Komora varuje před další vlnou podvodných mailů. (Pay the debts, this is a distress warrant. The chamber warns of another spate of fraudulent emails.)* Aktuálně.cz (online), October 19, 2015. http://zpravy.aktualne.cz/finance/falesne-exekuce-jsou-zpet-komora-varuje-pred-dalsi-vlnou-pod/r~cbdac6de765111e599c-80025900fea04/ (Downloaded: 15.08.2016)

[15] Phishing Activity Trends Report. *APWG* (online), 1st Quarter 2016. https://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf (Downloaded: 14.08.2016)

[16] PROSISE, C., MANDIVA, K.: *Incident response & Computer forensic.* Second edition. Emeryville: McGraw-Hill Companies, 2003.

[17] *Scam.* (online). www.businessdictionary.com/definition/scam.html (Downloaded: 11.06.2018)

[18] *Scam.* (online). https://en.oxforddictionaries.com/definition/scam (Downloaded: 11.06.2018)

[19] *Statistics of* CSIRT.cz. (online). https://csirt.cz/page/2635/statistiky-resenych-incidentu/ (Downloaded: 15.06.2018)
Statistics of the Police of the Czech Republic. (online). www.policie.cz/clanek/kyberkriminalita.aspx (Downloaded: 15.06.2018)

[20] VOLEVECKÝ, P., STACH, J.: Jak se krade pomocí Internetu – Phishing v praxi. (How to steal with the use of the Internet – Phishing in practice.) *Digital Doom's Digi World*, May 17, 2008. (online). www.ddworld.cz/software/windows/jak-se-krade-pomoci-internetu-phishing-v-praxi.html (Downloaded: 14.08.2016)

[21] KRUSE, P., HACQUEBORD, F., MCARDLE, R.: *Threat Report: W32.Tinba (Tinybanker) The Turkish Incident.* (online). CSIS Security Group and Trend Micro Incorporated, 2012. www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_w32-tinba-tinybanker.pdf (Downloaded: 15.08.2016)

[22] GEATER, J.: *Co znamená přípona souboru SCR?(What does the SCR file extension mean?)* Solvusoft (online). www.solvusoft.com/cs/file-extensions/file-extension-scr/ (Downloaded: 14.08.2016)

[23] HARNEDY, R.: *What is a Business Email Compromise (BEC) Attack? And How Can I Stop It?* Barkly (online), September 2016. https://blog.barkly.com/what-is-a-business-email-compromise-bec-attack-and-how-can-i-stop-it (Downloaded: 12.06.2018)

[24] DURAČINSKÁ, Z.: *Čo sa skrýva v prílohe podvodných e-mailov? (What is hidden in fraudulent email attachments?* CZ.NIT (online), July 23, 2014. https://blog.nic.cz/2014/07/23/co-sa-skryva-v-prilohe-podvodnych-e-mailov-2/ (Downloaded: 15.08.2016)

[25] *Zero-day (computer).* (online). https://searchsecurity.techtarget.com/definition/zero-day-vulnerability (Downloaded: 13.06.2018)

[26] *prikaz1B823F13856234527.zip* www.virustotal.com/cs/file/62170532b1f656c6917fa66d-0ed98462e106f3aa139273c9f2c3a370a67d265f/analysis/1471330723/ (Downloaded: 16.08.2016)

[27] www.csirt.cz/

[28] *Act no. 40/2009 Coll., Criminal Code.*