Ransomware

Jan Kolouch, Andrea Kropáčová

***Abstract*—**A combined attack, frequently referred to as ransomware, has recently become one of most common cyber attacks. This attack combines social engineering, malware attack and a criminal offence in the form of blackmail. The offender's aim is to gain a pre-defined "ransom" from as many end users as possible. Ransomware is a part of "malware economy" in which a number of similar attacks is launched with the aim of gaining profit from the victims. The article below defines ransomware and discusses the international legal liability for such types of attack.

***Keywords*—**Ransomware, cybercrime, Convention od Cybercrime, criminal liability, reverse analysis, social engineering.

I. Introduction

At present, combined attacks, frequently referred to as *ransomware*, have recently expanded dynamically. Such attacks cannot be easily defined as for instance a DoS or DDoS attack [1], [2], probe, scanning, hacking, or similar attacks. Ransomware attack combines elements of social engineering (luring the victim into downloading the infected file or visiting malicious websites), malware attack (infecting victim's personal computer and taking control over it) and criminal offence in the form of blackmail, the aim of which is generally to gain a pre-defined "ransom" from as many users as possible.

There is no doubt that ransomware can be classified as *internet organised crime*, or an element of the "malware economy". Ransomware in fact consists of a series of very similar attacks, the aim of which is to profit on as many victims as possible, irrespective of victim's location in the digital world, age, social background, education, etc.

II. Cyber attack

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 [3].

A cyberattack is deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyberattacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft [4].

Consequently, a **cyber attack**[1] 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 everyday life of the injured. A cyber attack can be either completed or it can be in preparation or attempted only.

Cyber criminality takes the form of cyber attacks. Cyber criminality is the crime in which IT technology is [4]:

a) *used as the tool to commit a criminal offence,*
b) *The target of offender's attack. The attack constitutes a criminal offence provided IT technology is used or misused in the information, system, programming or communication environment.*

Certain illegal action in the cyberspace or action related to cybercrime can be classified according to relevant provisions of country's regulations. There is, however, certain action that is difficult or impossible to classify as a criminal offence.

III. Ransomware

Many authors perceive **ransomware** as a type of malware. *Ransomware is a type of malware that prevents or limits users from accessing their system. This type of malware forces its victims to pay the ransom through certain online payment methods in order to grant access to their systems, or to get their data back. Some ransomware encrypts files (called Cryptolocker). Other ransomware use TOR to hide C&C communications (called CTB Locker) [5].*

Ransomware deploy malicious software which can disable the functionality of your computer [6].

Ransomware is malware for data kidnapping, an exploit in which the offender encrypts the victim's data and demands payment for the decryption key [7].

Ransomware that locks a computer and uses law enforcement imagery to intimidate victims has spread from Eastern Europe to Western Europe, the United States, and Canada over the past year[2]*. The scam has been copied and professionalized from initial early attacks, with established online criminal gangs now branching out into the scheme. Each gang has separately developed, or bought, their own*

= This work has been supported by the CESNET, a. l. e., http://www.cesnet.cz, operator of the Czech national research and education network referred to as CESNET2 within it "Large Infrastructure" (LM2010005) research programme of the Ministry of Education, Youth and Sports of the Czech Republic, running within 2010-2015 timeframe, .

Jan Kolouch works in CESNET, a. l. e., Zikova 4, Prague 6, Czech Republic, (email: kolouch@cesnet.cz).

Andrea Kropáčová works in CESNET, a. l. e., Zikova 4, Prague 6, Czech Republic, (email: andrea@cesnet.cz).

[1] A cyber attack does not correspond with the term **'security incident'**. A security incident is the violation of IS/IT security and the rules designed to protect it (security policy).

[2] Read Symantec report from year 2012.

different version of the ransomware. This malware is highly profitable, with as many as 2.9 percent of compromised users paying out. An investigation into one of the smaller players in this scam identified 68,000 compromised computers in just one month, which could have resulted in victims being defrauded of up to $400,000 USD. A larger gang, using malware called Reveton (aka Trojan.Ransomlock.G), was detected attempting to infect 500,000 computers over a period of 18 days. Given the number of different gangs operating ransomware scams, a conservative estimate is that over $5 million dollars a year is being extorted from victims. The real number is, however, likely much higher [8].

The above quote merely demonstrates the success and mass proliferation of cyber attacks that can be classified as ransomware. **Production and distribution of ransomware is directly linked to activities referred to as Crime-as-a-Service.** Over the past few decades the digital underground has evolved and matured from a few small groups hacking and phishing for fun and prestige, to a thriving criminal industry that costs global economies an estimated USD 300+ billion per year [9].

Crime-as-a-Service can be described as a business model (toolkit) which may include malicious software, supporting infrastructure, stolen personal and financial data and the means to monetise their criminal gains. With every aspect of this toolkit available to purchase or hire as a service, it is relatively easy for cybercrime initiates – lacking experience and technical skills - to launch cyber attacks not only of a scale highly disproportionate to their ability but for a price similarly disproportionate to the potential damage [10], [11].

Both from the professional and legal point of view, the above described actions represent a simplification of the complex process of the cyber attacks qualified as ransomware. This is why this article first deals with one of the best known ransomware – **"Police ransomware"**. Next, the punishment of the offender of the action with elements of ransomware within the framework of the international law will be discussed.

IV. "Police ransomware"

Since 2011, ransomware attacks on end user computers have taken place in almost every EU Member State. The aim of these attacks is to gain financial profit. The essence of the attacks is that the victim's computer is infiltrated with malware. Thus, the infected computer becomes a part of a botnet, through which the "blackmailing virus" spreads further. Subsequently, malware blocks access to the account of the OS Windows user while notifying him that the computer was blocked by the relevant country's police (see Figure 1).

In this case, the offenders seek to abuse people's trustfulness and "the appearance" of an official authority's communications to gain money from the users.

V. Legal aspects of ransomware

The core international document defining cyber offences is the Council of Europe's **Convention No. 185 on Cybercrime from 23 November 2001** [12]**.**

The Convention on Cybercrime constitutes the first international agreement in respect of criminal offences committed by means of information technologies (the misuse of the Internet and other computer network in particular) such as copyright infringement, computer fraud, proliferation of child pornography and other types of attacks against information and computer security. The aim of the Convention is to streamline the approach of Convention's signatories towards sanctioning the most serious types of cyber attacks.

From the legal point of view, a ransomware attack generally consists of the following actions:

1. sending an infected file, or a link to an infected website;
2. entering the malicious code in the computer;
3. data encryption in order to restrict the rightful user's access to the data or the system;
4. a request to pay a certain amount to unblock the computer or the data.

Figure 1 – An fake www page of Czech Police.

Ad 1. Sending an infected file, or a link to an infected website

The attack itself is de facto based on a phishing attack. Most frequently, the victim is sent an email which on the first sight does not raise any suspicion that it could contain a fake message. In general, such emails contain a link which the user is prompted to follow. Once the user has clicked on the attached link, he is directed to a website, the layout and functions of which do not differ from the authentic website. In reality, the user is redirected to a fake website which imitates the original more or less faithfully. Phishing collects data entered on the fake websites and sends them automatically to the offender. This way, the offender can obtain identification data of internet banking system's users or access to individual bank accounts of the users of the infected systems. The offender can also obtain identification numbers and other data relating to the payment cards which enable him to subsequently make payments through the Internet etc.

ISBN: 978-1-61804-320-7

During the ransomware attack, the user is not requested to make a payment or signed and administer secured accounts, etc. The aim of the offender is to persuade the user to visit the website on which the fake code is located. Once the user accesses this website, an attack on his computer is launched. This attack enables the offender to take over the control over the infected computer, to install malware to be able to control it distantly. Very often, the users' personal computers are attacked, compromised (e.g. by malware) and become a part of a *botnet*. The botnets enable generating massive DoS/DDoS attacks, or hide the activities of the offender and his identity in executing more sophisticated and precisely targeted attacks with a severe impact, see also [13].

Enclosing the fake code directly in the e-mail is another way to infect victim's computer. In such cases, the offender frequently misuses the default OS settings (mostly Windows based OS) enabling to hide the known file types. The victim for instance believes that he is opening a file in Word while his computer is being infected by means of malware (see Figure 2).

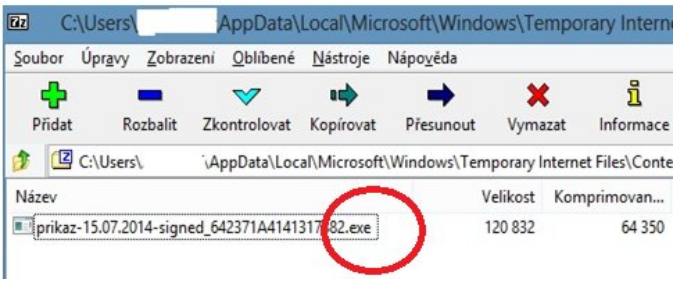

Figure 2 – An executable programme hidden as an order from a public authority

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 necessary cause damage the computer system (e.g. changing data in a database), this Articles 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 as 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 other, import, distribute or otherwise make available for instance malware (programme such as computer worms, Trojan horses, key loggers, etc) should be sanctioned. Article 6 of the Convention basically reclassifies the possession and handling of such programmes from an attempt to a completed criminal offence. This provision, however, does not provide for the sanctioning of the production of such computer programmes, unless the specific offender's intent (to commit any of the above listed criminal offences under the provisions of Articles 2 through 5 of the Convention) has been proved.

This provision should not be interpreted as if extending the criminal liability to each single disposal with the listed software. **For the criminal liability to arise, such tools should be possessed with the intent to commit any of the above listed criminal offences as defined in Articles 2 through 5 of the Convention**. Similarly, these provisions do not cover situations in which the protection of a computer system against malicious software is tested through a deliberate exposure of the computer system to such threats by the authors of the security measures.

Ad. 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 part.

It follows from the wording of the Article that the codification of the circumstances listed in domestic law is optional. Unless the circumstances are enacted as the indispensable condition for offender's criminal liability for the commitment of such criminal offence, a mere gaining of unauthorised access to a computer system or its part should be criminally punishable. Such regulation would enable to criminally punish for instance hacker attacks consisting of merely gaining the access to a computer system, even where the hacker's action caused no harm or where the hacker had not manipulated with data and information he obtained or got acquainted with during the attack.

Ad. 3. Setting a password on (hindering access to) rightful user's data

The action of the offender consisting in setting a password on (hindering access to) data to prevent the rightful user from accessing them can be classified as action described in Articles 4 and 5 of the Convention on Cybercrime. The merits of such action are deemed fulfilled once the user is hindered from a free use of own computer and data stored in it. The blocking of the computer itself is directly linked to the action described in paragraph below.

Ad. 4. Request for the payment of ransom to unblock the computer or data

The primary goal of the entire attack, shortly described as ransomware, is to gain financial profit for "unblocking the computer or data" for the compromised user. In general, the user is requested to send a certain financial amount, either through any of the payment portals (e.g. Ukash, paysafecard, MoneyPak, etc.) or through Bitcoin. Once the sum has been paid, a key (chain) renewing the access to the computer system or user data, is provided. However, malware level remains installed in the computer. Thus, the offender may repeat his request (blackmailing).

From the legal point of view, the above described action can be classified as blackmail, since the offender forces another person to act, neglect or sustain something. We presume that such action could be also subsumed under **Article 8 of the Convention on Cybercrime - Computer-related fraud.**

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 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 functionality of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.*

This provision defines a specific type of fraud, or more precisely a fraud committed in a specific manner – by interfering with computer data or computer system's functions.

The above described action, which according to this Article should be criminally punishable, occurs most frequently in conjunction with other action that the Convention aims to mitigate. For instance, the offender 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).

VI. Conclusion

Based on the above analysis, we believe that technical and legal professionals should cooperate more closely in the fight against cyber attacks or cybercrime. This would enable to revise the legal regulations of individual member states to sanction unwanted Internet action and to enable CERT/CSIRT teams[3] and law enforcement agencies in particular to fully exploit the means and the limits of the law to repress such illegal action.

References

[1] Andrea Kropáčová, (D)DoS attacks targeted web servers operated in Czech Republic, 17th International Conference on Computers: Recent Advances in Computer Science, Rhodos, 16 July 2013, ISBN: 978-960-474-311-7, ISSN: 1790-5109

[2] Jan Kolouch, "Criminal liability for DoS and DDoS attacks", 17th International Conference on Computers: Recent Advances in Computer Science, Rhodos, 16 July 2013, ISBN: 978-960-474-311-7, ISSN: 1790-5109

[3] PROSISE, Chris, MANDIVA, Kevin. *Incident response & Computer forensic, second edition.* Emeryville : McGraw-Hill Companies, 2003. p. 13. Compare also CASEY, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Second Edition.* London : Academic Press, 2004. p. 9 and further.

[4] KOLOUCH, Jan and Petr VOLEVECKÝ. *Criminal protection against cyber crime.* Prague: The Police Academy of the Czech Republic in Prague, 2013. ISBN 978-80-7251-402-1. p. 12.

[5] http://www.trendmicro.com/vinfo/us/security/definition/ransomware

[6] http://www.trendmicro.com/vinfo/us/security/definition/ransomware

[7] http://us.norton.com/ransomware

[8] http://whatis.techtarget.com/definition/ransomware-cryptovirus-cryptotrojan-or-cryptoworm

[9] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf

[10] http://www.mcafee.com/nl/resources/reports/rp-economic-impact-cybercrime.pdf

[11] https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta, page 20.

[12] http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1145.pdf, page 15.

[13] Convention on Cybercrime CETS No. 185: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ENG&NT=185

[14] Daniel Plohmann, Elmar Gerhards-Padilla, Felix Leder. *Botnets: Measurement, Detection, Disinfection and Defence.* [online]. [28. 3. 2014]. Available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/botnets/botnets-measurement-detection-disinfection-and-defence

[3] CERT = Computer Emergency Response Team, CSIRT = Computer Security Incident Response Team.