"New forms of cyber Attacks[1]"

Philippe Jougleux, Associate Professor, School of Law, European University of Cyprus

Tatiana Synodinou, Associate Professor, Law Department, University of Cyprus

Lilian Mitrou, Associate Professor, Department of Information and Communication Systems Engineering, University of the Aegean

Paper published in Proceedings of the 4th International Conference on Information Law and Ethics (ICIL), Thessaloniki, May 30-31, 2014

For as long as Internet exists, jurists and lawyers have tried to convince the public and sometimes we should add also themselves that Internet is not an outlaw region, a new far west whereas the civilization's rules cease to apply. However, now more than ever it has become obvious that every internet user is susceptible to become the victim of various forms of attacks from unknown sources, most of the time with unknown means and with any trace to the criminal.

While the terms virus, hacking and even cracking have become very familiar to the public, the new evolution of the cyber criminality's activity are for now much less known: what are exactly the romance scam, the scareware and ransomware? And what does it tell us about the actual mutations of the cybercriminal profile? This is the topic of this paper.

1

With the financial support of the Prevention of and Fight against Crime Programme European Commission – Directorate General Home Affairs. This project has been funded from the European Commission. This publication reflects the views only of the author, and the European Commission cannot be held responsible for any use which may be made of the information contained therein.

1. Evolutions of the legal framework: From the Convention of Budapest to the Directive 2013/40/EU

First, it seems fit to rapidly resume the applicable legal framework in EU to cybercrime. The notion of cybercrime possesses various definitions according to the scope of the research. By cybercrime we mean here what is sometimes called cybercrime *stricto sensu* or in other words the study of infractions which exists only through the use of computer systems. Therefore, this definition of cybercrime does not include the various violations of Intellectual property, the criminalization of speeches (i.e. hate speech) and the communication of images of child pornography. At an international level, the Convention of Budapest constitutes certainly a major step in achieving a harmonization and modernization of the national legislations of European countries, since it has been created under the supervision of the Council of Europe, but not only. For instance, Canada, Japan, Usa, South Africa have signed also the Convention.

The European legislator also has decided to intervene in this field with first a decision-framework on 2005[2] and then with the EU Directive of 2013 which replaces it[3]. As described in a communication of the Commission of 2008, this new reform was judged indispensable in order to "combat the use of botnets for criminal purposes and to promote the use of the same contact points used by the Council of Europe and the G8 to react rapidly to threats involving advanced technology"[4].

Nevertheless, the fundamental structure of the legal framework of the cybercrime *stricto sensu* has not been discussed since the Budapest Convention. It takes the shape of a basic division between four offenses: illegal access, illegal interception, data interference and system interference.

This division can sometimes be tricky to apply to the various antisocial phenomena which exist on Internet. For instance, some viruses, such as for instance a keystroke logger (software which records what keys are stuck on a keyboard), are installed through an illegal access to the core component of a system, while they modify the security option (date interference and system interference) with the goal to gather data about the user by saving his

[2] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.
[3] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.
[4] Commission Report to the Council on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems, COM(2008) 448 final.

interaction with the system (illegal interception). Anyway, this distinction has prevailed also at the European level.

Indeed, this distinction has the merit to analyze at a conceptual level the nature of the criminal threat and therefore to show the necessary elasticity in order to adapt to the constant mutations of the cybercriminal activities. It focuses on the concept of authorization: the illegal access and the illegal interference are defined as the access or the interference by violation of the will of the legitimate user of the system or right holder of the data. The lack of authorization is proven by the use of technical means which circumvent the various protection measures of the system.

2. New threats, old threats

2.1. New, evolved Romance scams: the webcam blackmail

Romance scam could be broadly defined as the use of identity theft as a mean to exploit the feelings of the victim and acquire some monetary advantages. Whereas romance scam existed even before internet, it has recently mutated in a very serious threat and a successor of the famous Nigerian scam of the past in the mind of the cybercriminals. Indeed, the classic romance scam, just as another form of Nigerian scam, is mostly based on phishing through email and therefore the internet users have constantly grown aware of its existence and have learned to avoid its danger.

At the opposite, the new kind of Romance scam uses the most modern communication tools of the Internet. The attack could be processed in four stages: first, the cybercriminal installs its identity theft on a social network, either general or specific for dating services, by using several images, video and other personal data of models or just real innocent persons. Then, either the victim or the cybercriminal will take the initiative of a contact, of a communication which would conclude in a rendezvous on a chat room. In the stage three, the communication evolves in the use of a webcam. Using a small technological trick, the cybercriminal only plays a preloaded webcam video footage instead of a real streaming image and persuades the victim to be involved in a by distance sexual practice. The video discussion of course is recorded and after some minutes the blackmail stage starts, with a combination of hacking of the list of contacts of the victim: “I have all your contacts’ emails. If you don’t pay within 2 hours, I send them the video”.

In consequences, the very sensitive content of the blackmail assures a high level of success, whereas at the same time neutralizes the fear of an encounter with the repression forces. As a last line of defenses, the cybercriminal will hide behind his anonymity. Characteristic also of this new trend is the high level of emotional damage involved. It was only sadly a matter of time before this scam to have some dramatic effect, as, for instance, the suicide of a 17 year old teen last year[5].

From a legal point of view, the relevant issues are by consequent both on criminal law to find a way to enforce the legislation about fraud, extortion but also about personal data protection, by developing anonymous forms of plaint and fast intervention units, and on civil law to find a way to estimate the moral damages of this activity. The eventual intermediaries, even if protected against liability by the famous safe harbor, should contribute to the protection with a better identification of false profile.

2.2. The Ransomware and scareware

The ransomware is certainly one of the most disturbing evolutions of the cyber criminality. On the essence, it's just a category of virus like any other virus which existed before, but with the difference that it does not destroy the data but encrypt them. Therefore, it gives to the victim the hope to retrieve the data, by paying a sum through an electronic method of payment like bitcoin usually. Typically, a message appears suddenly and warns the user that his hard disk has been encrypted and that he has 3 hours to pay the "ransom" in order to obtain the encryption key which will "liberate" the data.

Now at a legal level, it is not peculiarly difficult to find an offence: data interference, system interference, fraud, money extortion. The main issue is at the enforcement level: the so called "black number" of the criminality, in other words, the difference between the real numbers of the cyber criminality and the declared cases is already huge. The main causes of the black number are classically the innocence, the unawareness of the shame of the victim. Now, in case of the ransomware, the enforcement will become ten times more difficult, since the criminal plays with the victim's hope to retrieve some precious data that are kept only on the hard disk.

Similarly, the scareware is based on the appearance of the ransomware. At the difference of the ransomware, there is no real treat to the system or the data, but a message appears

[5] See: Teenager's death sparks cyber-blackmailing probe. Available at: http://www.bbc.com/news/uk-scotland-edinburgh-east-fife-23712000.

which aims to convince the user of the contrary. The aim is to force the user to pay scammers for a bogus service which allegedly would protect them from the treat. In the same way, the criminal uses also – one could say quit cleverly – the guilt and fear related to the massive use of pirated cultural product. A message appears and explains that the special internet force of the police have found him for IP infringement and in order to avoid judicial consequences a fine has to be paid to a specific account.

At a legal level, one issue is not to find an applicable offense, but to deal with the plurality of offenses: according to the national legislation, the offense of fraud or illegal extortion will outstrip the offenses of illegal interference. And once again, the main difficulty lies in the enforcement procedure.

2.3. New Adware's generation

In the same way, some disturbing new trends have to be noticed in the field of adware. While classic adware were very obvious, creating new windows full of apps, the new generation of adware aims to modify the behavior of preinstalled software on the system by inserting a layer of ads on websites or covering up other paying ads. It works more commonly as a kind of parasite infection of a browser program or on an Operating System. In this evolution, the adware just replace a true, legal advertisement, with another one, either in the specific banned pages of website like Facebook or even in the search results of some famous search engines as Google[6]. By consequence, obviously, the first victim will have some difficulties to understand the reality of the attack since it does not suffer any pecuniary damage or apparent loss of amenity. However, a multiplication of these new adware could undermine considerably the net economy, by withdrawing the main amount of income from a lot of websites whose revenues is based on advertisements. Whereas the classic adware business is now part of the Internet history for some years already[7], this success of the anti-adware forces was based mostly on the so called "lousy consumer experience". Even when adware doesn't carpet bomb users with ads, it is still largely based on interruption marketing

The first line of defense of the companies behind these adware is that since they are not themselves users of the infected website, they are client-side software and by consequence

[6] E. Steel, New 'Adware' Apps Bug Facebook, Google, December 9, 2011. Available at: http://online.wsj.com/news/articles/SB10001424052970203413304577086463731021828.
[7] E. Goldman, Adware is Dead. Long Live Adware!, May 1, 2008. Available at: http://blog.ericgoldman.org/archives/2008/05/adware_is_dead_1.htm.

they are not bound by their policy. However, it can be denied really that these adware correspond to a form of unfair competition.

3. New organizations, new motivations, new profiles

3.1. The state involvement

The Budapest Convention, as the EU Directive of 2013 leave in the dark a matter which have become lately very sensitive. Even if nowadays legal persons can be found guilty of cyber-attack by application of the Article 10 of the Directive 2013/40, nobody has foreseen or wanted to prepare to the multiple offenses committed by States themselves.

For instance, State involvement in the virus creation has been found in the creation of the Stuxnet virus[8] which was a dormant virus, until it touched the Iranian nuclear complex. Strong suspicion exist that the Israel service named "Unit 8200" is involved in its creation, in collaboration with the USA and Edward Snowden confirmed it in an interview in 2013. The difference with classic operation of sabotage is that the virus Stuxnet, to be operational, has to infect a wide range of computers and by definition to infect a lot of innocent users.

In the same way, the State involvement in mass surveillance of the Internet users has made the head titles of the newspapers for almost 2 years now, with the revelations about the NSA programs of data interception. Either with some computer programs such as PRISM, Xkeyscore, Tempora, Muscular or with secret treaties such as Project 6, Stateroom, Lustre the NSA intercepts huge amount of personal data. From a legal point of view and in a European approach, these revelations create some difficult issues. In a criminal procedure, the prosecutor will have to discuss the jurisdictionally and according to the article 12 of the Directive 2013/40 he will have to prove that the offense has been committed either within the territory of EU, either by an EU citizen (and if his act constitutes an offense where it has been done). A cybercrime is committed within the territory of EU according to the second paragraph of the article 12 whereas the offender is physically present in the EU or the attacked information system is hosted in the EU. However, when the USA collects data directly who transit through their territory or from one of the immerged atlantic cables, it is difficult to determine a jurisdiction in EU. On a civil court, one plaintiff would also have to surpass some impossible obstacles, such as to give to proof that he was indeed one of those millions of users whose communication data have been intercepted.

[8] See: http://en.wikipedia.org/wiki/Stuxnet.

Also, the State involvement in Cybercrime means to analyze the State as a victim itself of cybercrime. The EU institutions had already shown their interest in this domain with a Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 30 March 2009 on Critical Information Infrastructure Protection[9] and two years later, with another Communication on the same topic[10]. The main idea is to distinguish a classic illegal access to an automatic system from the more dangerous illegal access to a critical information infrastructure, such as a water or electricity supply computer system or a mass transportation management system.

3.2. A cyber-mafia

The Distributed Denial of Service attack (DDOS) is often described as the most brutal kind of attack. It is quit the most efficient somehow, since there is really no efficient protection against it. It operates by connecting a huge number of computers to one system, flooding it with request of connection, hoping that the demanded resources will surpass the system's bandwidth and ultimately freezing it. The only solution for the big companies is to add a lot of servers in order to be able to respond to this threat. In practice, the pirate will act not personally but through a park of "zombies" computers, a park of vulnerable computers (in libraries, public offices, internet cafes, etc..) infested with a Trojan horse which gives to the pirate a full access to it.

At a legal level, even if there is no violation of technical measure, there is no doubt that the DOS attack is contained in the definition of the offense of illegal interference of a system as defined by the new Directive 2013/40. It was one of the main purpose of the reform to incorporate the repression of the DOS attack. The text explains indeed that illegal interference is committed even without access to the system whereas it has the consequence to disturb the normal functioning of the system.

The new treat and the issue here is not therefore the existence of the DOS attack itself but its exponential uses in various contexts. Nowadays some Dos attack rental service have appeared, which means that the hacker put its botnet park to the disposition of some clients,

[9] "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" [COM(2009) 149 final.

[10] Communication of 31 March 2011 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 'Achievements and next steps: towards global cyber-security' [COM(2011) 163 final.

through remuneration. The ideological motivation of the hackers in the past have been replaced in a large scale by a more classical motivation: the money. Nowadays, with 5 dollars on hour, anybody can discretely (with payment through bitcoin) ensures that the ecommerce model of his competitor is paralyzed. The issue here is as always the enforcement. Nevertheless, the client, if found, would be subject to the article 8 of the Directive 2013/40, which provides that the incitement, or aiding and abetting, to commit a cybercrime is punishable as a criminal offence.

3.3. The cellphone as a target

According to the first article of the Directive 2013/40, an information system "means a device or group of inter-connected or related devices, one or more of which, pursuant to a programme, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance". There is no doubt following this definition that a cellphone is device processing computer data, however until recently the limited capacities of the phone was the main technical obstacle to the proliferation of cyber-attacks. Obviously the situation has radically changed now and cellphones have become a main target of cyber-attacks.

The most logical peoples' concern of surtaxed calls through a malware application should not be seen as the most important and new threat. From one hand, the hacker ensures quickly a large benefit from the surtaxed calls. But from the other hand, in this domain the enforcement of the law is deemed to be easier for the special police unit in charge.

However, the cellphone is particularly vulnerable to a wide range of attacks, from the interception of communication and privacy issues (remote access to the camera or the microphone of the phone), to more original malware. For instance, The virus BadLepricon is an application that can be downloaded through the playstore interface of android and it is very characteristic of the new threats posed by the virus. This app exploits the calculation resources of the cellphone while it is apparently sleeping in order to create some electronic money. Basically, it does not constitutes an illegal access, since it has been installed with the consent of an innocent user. The app also does not interfere with the data and personal data of the cellphone. But the use without consent of the calculation resources of the cellphone, with consequences such as a diminution of the battery capacities, should be ruled as a form of illegal system interference. At the opposite, Google will be protected by the intermedia-

ries' safe harbor with the condition that it promptly remove the malware from its database of applications once it had been alerted.

4. Conclusions: which solutions?

It is certainly quit easier to point out the issues than to offer solutions. From the Budapest Convention to the new Directive, the focus has always been put to two axes of enforcement: international collaboration and procedural adjusting. For instance, a European agency has been found and national contact points created, which are accessible 24 hours a day. The new threats analyzed here should most certainly urge to an amplification of these interactions. For instance, the contact points should be open to the public, which could easily and most important quickly alter the authorities about an offense. Also, as we have seen, most of the new offenses have a pecuniary motive and a reflection has to be made on the regulation of the so-called crypto-currency.