

eNAC

The Cybex Initiative | e-NEWSLETTER ON THE FIGHT AGAINST CYBERCRIME



LEGAL

Katalin Parti from the Hungarian National Institute of Criminology explains the actual importance and future evolution of alternative report hotlines.

DATA PROTECTION

Ricard Martínez from the Spanish Data Protection Agency highlights a peculiarity of Spanish data protection legislation that applies to the possibility of proving certain types of conduct.

TECHNICAL

Eddy Willems from KASPERSKY LAB explores what actually happens during a drive-by attack, the lures used to perpetrate attacks, the technology behind the attacks, and the use of drive-by download attacks in personal data theft and computer takeovers.

LAW ENFORCEMENT

Interview with Bernhard Otupal from INTERPOL, the world's largest international police organization, which facilitates cross-border police co-operation among its 187 member countries.

INSTITUTIONAL

Interview with technical expert Raoul Chiesa from UNICRI to reveal how this Institution fights against cybercrime.

JURISPRUDENCE

The cases summarized below in this issue consider how people use digital devices to conduct business, and how the legal requirements of form imposed by politicians is either ignored or not known (the latter is probably the actual reason).

EVENTS

Selection of conferences for the months of September and October 2009 that might be of benefit to lawyers, prosecutors, technicians, judges, computer forensic specialists, law enforcement bodies or any person that deals with cybercrime and electronic evidence.



Criminal Justice 2008

With financial support from Criminal Justice Programme
European Commission - Directorate - General Justice, Freedom and Security



The Digital Forensic Company

✘ INTRODUCTION

We would like to thank you for all your positive comments regarding this newly born publication, the Electronic Newsletter on the Fight Against Cybercrime (ENAC), which presents today its third issue.

◎ LEGAL

“The importance and future of alternative reporting hotlines”

Katalin Parti • Research fellow with the Hungarian National Institute of Criminology

✘ DATA PROTECTION

“Evidence of illegal conduct in databases subject to compliance with high-level security measures in Spanish legislation”

Ricard Martínez • Coordinator of the Study Area of the Spanish Data Protection Agency

🔗 TECHNICAL

“The increasing problem of drive-by downloads”

Eddy Willems • Security Evangelist at Kaspersky Lab and EICAR

✘ LAW ENFORCEMENT

“Threats of cybercrime and INTERPOL's response”

Interview with Bernhard Otupal • Assistant Director of INTERPOL's Financial and High Tech Crime Sub-Directorate

○ INSTITUTIONAL

“United Nations & UNICRI in fight against cybercrime ”

Interview with Raoul Chiesa • Cybercrime Issues & Strategically-Related Alliances - Technical Contact - UNICRI

↑ JURISPRUDENCE

Greece · Court of first Instance of Athens

China · Beijing Hai Dian District People's Court

Belgium · Ghent Court of Appeal, Chamber 7bis

Sri Lanka · High Court of the Western Province

□ EVENTS

Conferences, events, trainings and seminars related to cybercrime, electronic evidence and computer forensics.

◎ EDITORS

Introduction of the team of seven editors that has been engaged to create the Electronic Newsletter on the Fight Against Cybercrime, each one being an expert on the ENAC Section of which they are in charge

↑ DISTRIBUTOR PARTNERS

To ensure the widest possible distribution of the Electronic Newsletter on the Fight Against Cybercrime, the ENAC relies on the collaboration of Institutions and Organizations who will distribute the e-Newsletter monthly to their contacts database.



e)NAC

E-NEWSLETTER ON THE FIGHT AGAINST CYBERCRIME

Dear readers,

We would like to thank you for all your positive comments regarding this newly born publication, the **Electronic Newsletter on the Fight Against Cybercrime (ENAC)**, which presents today its third issue.

It is a pleasure for the ENAC team to realize that its objective of producing an e-Newsletter which provides, from one hand, a professional approach on the current problem of cybercrime from different perspectives -legal, data protection, technical, law enforcement, institutional and jurisprudence-, and on the other hand, the exchange of information and share of knowledge between professionals and updates on electronic evidence legislation around the world is being successfully accomplished.

But the effort being done by the **ENAC** team, **Cybox**, and the **European Commission's Directorate General Freedom, Justice and Security** would be senseless without a close relation with the project cornerstone, our readers. The ENAC has been thought, developed and prepared for you, so from the ENAC team we would like to welcome you to send us your feedback, your ideas or your requests so that they can be evaluated and taken into account.

We truly appreciate your support!

Enjoy the read,



Mrs. FREDERICKA INSA
Project Director
finsa@cybex.es



Mrs. MIREIA CASANOVAS
Project Coordinator and Chief Editor
mcasanovas@cybex.es

Cybox
Plaza Cataluña 20, 9ª floor · 08002 · Barcelona · España
tel. +34 93 272 20 41 · fax. +34 93 215 50 72

[Go to Russian version of the ENAC](#)

[Go to Spanish version of the ENAC](#)



Criminal Justice 2008

With financial support from Criminal Justice Programme
European Commission · Directorate · General Justice, Freedom and Security



The Digital Forensic Company



KATALIN PARTI

Research fellow with the Hungarian National Institute of Criminology



THE IMPORTANCE AND FUTURE OF ALTERNATIVE REPORTING HOTLINES

Katalin Parti is a PhD, a research fellow with the Hungarian National Institute of Criminology. Her major research fields are cybercrime, criminal law as a regulating tool of cyberspace, application of criminal forensics in cyberspace cases, virtual communities, online sexual abuse. Contact: parti@okri.hu. Web: <http://en.okri.hu/content/view/51/82/>

1. Introduction

These days, there are two important changes in how victims are perceived. One of the changes involves the widening scope of the definition of victims, while the other is linked to the development of the internet, which influences how victims are treated.

Nowadays, the definition of a victim does not solely correspond to the definition under criminal law - that is a person who suffered direct harm or damage in relation to a crime -, but rather all persons are to be regarded victims, who suffered direct or indirect, physical or mental harm or inconvenience in relation to a criminal act. Several conventions of the European Commission, EU documents¹, and legal regulations on a national level pertaining to compensation by the state² apply this wider definition.

As for the development of the internet, the European Parliament and the Commission have already become aware of the dangers related to the development and spread of the internet and online technologies in the mid-1990s, and from 1999 launched action plans for more secure internet use³. The last action plan was approved in 2008, which is expressly aimed at the protection of children, who are the most frequent users of the internet⁴. The Council of Europe's Convention on Cybercrime opened for signature on November 23, 2001 in Budapest can also be regarded as a milestone in the fight against harmful internet contents. The convention stipulates the creation of internet hotlines in the member states with 24/7 availability, which ensure the exchange of information needed for international cooperation in criminal proceedings.

The widening definition of victims also extends the role of hotlines, in that not only direct victims, but everyone may report physical and virtual offences there.

¹ Besides the United Nations and the European Commission, the European Union also deals with helping victims of crime and compensation, and several related documents aimed at the governments of member states have been accepted. Such are for example the European Convention on the Compensation of Victims of Violent Crimes passed by the Council of Europe on November 24, 1983; the conclusions of the Tampere European Council of October 15th and 16th, 1999, especially paragraph 32; and the European Council's Framework Decision of March 15th, 2001 on the standing of victims in criminal proceedings. According to the provisions of these documents, the member states have to appropriately regulate the access to justice of crime victims, and the enforcement of their claims for compensation. On April 29th, 2004, The European Council has issued directive 2004/80/EC relating to compensation to crime victims. Under the directive, from January 1st, 2006, all member states of the EU have to provide compensation to all EU citizens, if they fall victim to premeditated and violent crimes in the given member state.

² Such is for example Act 135 of 2005 of Hungary on crime victim support and state compensation. EU legislation fundamentally does not affect the rights of member states to create their system of state compensations according to their own legal tradition, and social and political considerations. However, they have to guarantee that a victim, who initiates proceedings for compensation in a member state other than his own, should receive the same treatment as EU citizens who are residents of the given state, and that difficulties arising from the cross-border nature of the case should not impede the compensation proceedings.

³ These were the Action Plan for a Safer Internet (1999-2004), and the Safer Internet Plus Programme (2004-2008); decision No. 276/1999/EC of the European Parliament and of the Council (January 25th, 1999); and decision No. 854/2005/EC of the European Parliament and of the Council (May 11, 2005) adopting a multiannual Community action plan promoting safer use of the internet and new online technologies.

⁴ Decision of the European Parliament and of the Council establishing a multiannual Community programme on protecting children using the internet and other communication technologies (February 27th, 2008) (COM(2008) 106 final)



2. Definitions

In this article, I use the term "alternative reporting hotlines" not exclusively in the sense of services offered to crime victims, but rather hotlines developed for the broader public, which enable any person who directly or indirectly encounters crime, or deviant behaviours causing disturbance to communities to report those.

From this point of view, a grandmother who, being an inexperienced internet user, often encounters offensive online contents can just as well be a victim, as well as a parent or teacher, who reports an illegal or harmful website out of concern for the mental health of children under their care.

What makes these hotlines alternative, or unusual? I use the adjective 'alternative' to distinguish these hotlines from traditional forums. While traditionally crimes could be reported by the victims themselves in person, alternative hotlines can offer impersonality. The two communicating parties, the person reporting, and the person receiving the report are not in physical proximity, which makes their contact impersonal. Impersonal, because no personal characteristics of the reporting party can be seen, and the person receiving the report also answers impersonally. It is in this respect that alternative reporting hotlines, whose medium is mostly the internet, differ from traditional, real-time places of reporting which either demand personal appearance, or a phone call.

We can distinguish between alternative reporting hotlines which only receive reports of illegal and harmful internet contents (such as for example the international hotline-system of Insafe)⁵, and those that receive reports of any online or offline forms of deviant behaviour (such are for example the mental health support centres which originally only accepted reports in person or by phone, or the police's telephone or internet hotlines).

3. The importance of alternative reporting hotlines

It may sound surprising, but the advantage of alternative hotlines lies in their impersonality. Victims of violent crimes against persons prefer to remain "hidden". It is perhaps for this reason that they have more trust in alternative hotlines, as they can remain faceless⁶. They do not have to be afraid of the retaliation of their attacker, and can still receive personal care. Establishing such a contact is easier, the assaulted party has less psychological blockages to battle until they finally contact the hotline and ask for help. Alternative reporting hotlines also raise user-awareness. They promote the reporting of such behavioural forms that may not qualify as illegal, but still adversely effect the interests of certain groups. Typical examples for these are for instance harmful internet contents that even though they are not criminalised⁷, they pose a threat to the healthy sexual and moral development of children. Such harmful contents are available on the internet in such great abundance that fighting them can not be a solitary mission.

⁵ Insafe: the European network of e-safety awareness nodes. <http://www.saferinternet.org/ww/en/pub/insafe/index.htm>

⁶ In the case of violent crimes against persons and especially sexual offences, victims' willingness to report is usually very low, exactly because of the "hiding" behaviour of the victim. The victim of the crime attempts to protect themselves from further harassment in that they avoid all human contact. At the same time, it is exactly the victims of crimes that invade the private sphere to such a huge extent, who would require the most external assistance to help them cope with the trauma of the crime.

⁷ The European Union distinguishes between illegal and harmful internet contents. Contents that pose a threat to a certain layer of society, such as children, are regarded as harmful, while all contents are considered illegal that are criminalised by the member states. For a detailed description see the decision of the European Parliament and of the Council establishing a multiannual Community programme on protecting children using the internet and other communication technologies (February 27, 2008) (COM(2008) 106 final) p. 4

Protective measures, however, should involve more than just reporting actual crimes. The reporting of harmful contents not classified as criminal should be promoted, which can be most easily achieved with the development of easily and quickly available alternative reporting hotlines open to everyone. Alternative hotlines are also a great tool for community building as they raise the users' awareness of threats. They enhance the feeling of responsibility for others, and they contribute to the development of community altruism.

Online psychological counselling, online psychotherapy, online mediation, and the development of virtual communities for personality development are only a step away from the above. Psychology has recently discovered the potential of online counselling. Due to the inherent facelessness, it is a lot easier to get into contact with someone on the internet. At the same time, the lack of verbal communication, and the growing importance of written communication helps towards the delineation of problems and the revelation of underlying realities. We know of virtual communities, whose main activity is self-help to their members. These communities get organised very quickly, ensure quick development due to their anonymity, and the shared problems become more apparent. Those who need specialist help, will also find the related forums more quickly, as the exchange of information is more rapid. These virtual problem-solving communities also make use of the preventive and self-helping effects of internet communication.

4. Problems of alternative reporting hotlines

Paradoxically, the disadvantages of alternative hotlines almost all arise from their advantages. For example, the possibility of anonymous reporting may prevent the police from acquiring further information about the case essential for launching proceedings. At the same time, the quick and easy access of alternative hotlines may start a flood of mass reports. This in itself would not be a disadvantage. But at any rate, the authorities will prioritise their actions according to the gravity of reported cases. This in turn might prevent them from taking action in each and every case, and may lead to the cases becoming trivial. The true disadvantage of alternative hotlines today is the low level of development, both in terms of technical background and personnel (attitudes). The operators of hotlines - NGOs and the police - leave most of the reports unanswered. This phenomenon, namely the denying of crimes by the authorities, and the bagatellisation effect greatly contributes to the waning trust in authorities, or the complete lack of it. Research has found that an automated response to reports is still better than rewarding the efforts of the reporting person with no response at all. The response may be minimal, and may limit itself to information about the forwarding of the report, but it is essential for enhancing people's trust in the authorities (or hotlines). A simple response from the hotline may increase people's willingness to report, and may reaffirm the feeling of responsibility for the community⁸.

There is also another approach to alternative hotlines, namely from a jurisdictional, or e-justice aspect. Mediation, the wider definition of victims, and promotion of the dialogue between perpetrators and victims have become an integral part of jurisdiction.

⁸ One of the conclusions from the workshop on March 27th to 29th, 2008 in Preston, UK on the role of the internet in jurisdiction was that the former Soviet satellite states build a show of appearances in setting up online reporting hotlines. This basically means that the hotlines are not functional. Their primary function is to reassure the reporting persons with a response, they are not updated, static, and they do not provide sufficient information to citizens to raise and confirm their personal responsibility. The situation in Eastern European countries is partly worse than in Western Europe, because in Eastern Europe, authorities were a tool for the legitimisation of power, and keeping order. In new democracies, this role of the servant of power and retaliator has not been fully replaced yet by the helping and community building role. One of the consequences is the underdeveloped status of hotlines based on a sense of responsibility for others, and the lack of trust.

The development of the sense of responsibility of both individuals and communities, the promotion of community action and the willingness of individuals to protect themselves based on a heightened awareness of threats are incorporated into the European Union's jurisdiction and action plans⁹. The aim of the safer internet programmes (1999-2004, 2004-2008) was raising the threat-awareness of communities, and the development of cooperation between communities and the police (community policing of cyberspace, essential public/private partnership, the community policing concept). This approach was adopted by the Safer Internet Programme (2009-2013) of the European Parliament and of the Council¹⁰, which promotes action against internet contents harmful to the healthy development of children, rather than against harmful internet contents in general. Localised and customised individual programmes must be created on a local level, which are best suited to address the problems of the given community. The main tools of prevention is raising awareness in society and creating knowledge-basis, which include self-control on the users' level and are raising the awareness of possible threats. Filter-software solutions need to be developed that are technically capable of filtering harmful contents. As part of this strategic partnership, the importance of alternative hotlines will grow.

We can see that reporting hotlines are in need of further development also if we consider that their operators put no efforts into prevention, and they do not cooperate in strategic programmes for prevention. Hotlines operated by NGOs, and the alternative hotlines of investigative and consumer protection authorities have no knowledge of each other, or do not acknowledge each others' activities. Information exchange is poor, and there is no network organisation to talk about. The hotlines do not communicate with each other, and have no information about the future treatment of reports that they may forward to each other. They compile no statistics about the reports they receive, even though they could use them to elaborate prevention strategies (what online attacks may be expected against what companies, what technical and personal threats do users face in simple online communication, etc.). Raising the threat-awareness of users could be a tool of primary prevention. This, however, is not realised, as hotlines are difficult to access¹¹ and provide little information to users.

5. The further development of hotlines: A bright future?

Even though, despite the lack of personal contact to the helper, internet hotlines have a lesser importance in dissolving psychological conflicts, they are wonderfully suitable for forming small problem-solving communities. Those victims, who do not want to uncover their identity, will find it easier to enter into contact with the expert in charge of the therapy exactly because of the lack of personal contact, as they are held back from asking for help personally by their feeling of shame. Internet hotlines could be developed further so that they could offer instant minimal support to the victims, such as by a simple response (what happened to their report, where else they can turn, where they can receive information about the proceedings launched in relation to their report). More and more psychologists have online sessions now. Establishing a contact with the psychologist is easier, as the person asking for help does not appear in person, and therefore has less inhibitions to fight. At the same time, the written formulation of problems promotes the identification of underlying truths.

⁹ See n^o8.

¹⁰ Decision of the European Parliament and of the Council establishing a multiannual Community programme on protecting children using the internet and other communication technologies (Brussels, February 27th, 2008) (COM(2008) 106 final)

¹¹ For example the largest internet hotline in Hungary set up for reporting harmful internet contents is a member of Insafe, the international network of hotlines, but it is only available with 8 to 10 clicks, after targeted conscious searching, so it is not well known. There are several websites aimed at raising children's awareness of online threats, such as the Kék-vonal (Blue Line) and the website of the Hungarian Commission for Crime Prevention, but they do not "jump to the eye" either. A child spending more than 3 hours a day online will not spend his time searching for websites raising threat-awareness, but more likely with establishing friendships, looking for friends, socialising, or searching for information needed for their homework. (Kerezsi & Parti, 2008: 130-131; World Internet Project 2007, TÁRKI-ITHAKA)



Often enough, formulating the problem well is the first step towards recovery. Besides that, virtual communities may help the individual's recovery in that they attract members with similar problems, who will help each other.

So called second realities are virtual worlds, where the participants may choose their identity after registration: they can choose their physical appearance and build their personality. The chosen identity is often fundamentally different from the real personality. These virtual communities (e.g. Second Life) offer us the opportunity of living out the hidden reserves of our personality, of finding friendships, building communities or even earning income. Virtual communities are attracting more and more users due to the freedom of self-realisation and creativity. As they have great community-organising potentials, they are suitable for the creation of self-helping communities.

Besides second realities, which are entirely a product of the imagination, teleimmersive and augmented realities merging the online and offline worlds (both objects and persons) are becoming increasingly popular these days. While teleimmersive presence means the virtual extension of physical space (with computer-generated, imaginary objects and persons), augmented realities focus on adding virtual elements to physical space¹². In virtual reality, the world of fantasies is expressed increasingly more realistically, so much so that the boundary between imagination and reality almost seems to blur. This schizoid condition was only possible to achieve with hallucinogens or transcendental meditation in the past, but computers do the job for us now. The development of computer technology projects a future in which dealing with victims may become more effective. In the teleimmersive or augmented realities, the victim in need of help may get into contact with the virtual community or their psychologist through a virtual alter ego. This way, there is personal presence, but a more effective protection of the private sphere is also ensured. These technologies, however, may not only be used in psychological counselling or building online communities, but also in everyday administration. Let us imagine virtual public administration portals (virtual client gates), where the administrator and the client are both represented by their virtual alter egos. This not only guarantees quick and simple administration, but also eliminates the possible distrust for the authorities. As a result, there may be more reportings, and less deviance remains in the "dark zone" (latent). The virtual presence of the administrator (policeman, lawyer, legal expert, psychiatrist, etc.) lends intimacy to the conversation and the reporting party receives instant feedback, which helps promote trust, and enhances the feeling of responsibility for the community.

The fact that helpers of victims and people working in public administration and jurisdiction have no direct interests in the use of virtual technologies may prove a hindrance to virtual administration or consultations. Generations born before the 1990s, before the spread of the internet, did not experience computers and the internet as a fact of life, which often has the result that they are unwilling to learn the skills needed for their operation. In jurisdiction, technologies needed for probative force, such as electronic signatures are not wide-spread, as they are still very expensive. While public administration processes are highly automated (electronic client gates), the use of computer tools and technologies in jurisdiction has only just started. In Hungary for example, online reports sent to the police, are first printed, and then forwarded to the responsible and competent local investigative authorities by fax.

¹² Augmented reality applications usually demand the use of some technical aid, such as 3D-headgear or glasses. The appearance of virtual reality applications merging telepresence and virtual reality technologies can be expected in the early 2010s. Augmented reality technologies are used in entertainment, learning, and as a support for medical work. See Max Planck Research. Science Magazine of the Max Planck Society. 4/2006 http://www.mpg.de/english/illustrationsDocumentation/multimedia/mpResearch/2006/heft04/4_06MPR_gesamt.pdf



The means for the electronic recording, authentication and applicability in front of the court of evidence are available, but in practice, they are not widely used.

For the development of the so called e-justice, and the online management of victims, not only the attitude of the participants needs to be changed, but the technical tools also need development. Basically, it is still the lack of broadband internet access which stands in the way of the idealistic vision of the future I describe here. Broad-band internet access is still necessary for virtual presence, and for the virtual communication of victims and helpers. But this is exactly what is out of the reach of those people living on the edge of society¹³.

References

Parti, K. (2008). Számítástechnikai devianciák. (Computer deviances) In Kerezsi, K. & Parti, K. (Ed.) *Látens fiatalkori devianciák. Fiatalkori devianciák egy önbevalláson alapuló felmérés tükrében - "ISR-D-2" (Latent deviant behaviours in youth. Deviances in youth in the mirror of a self-reported survey)* Budapest: OKRI-ELTE

Kék notesz 2007. A 8. internethajó jelentése. eWorld & ENAMIKÉ, 2007. április 19. (Blue notes 2007. Report of the 8th InternetBoat) http://internethajo.hu/media/Internethajo_Kek_Notesz_2007.pdf

Max Planck Research. Science Magazine of the Max Planck Society. 4/2006
http://www.mpg.de/english/illustrationsDocumentation/multimedia/mpResearch/2006/heft04/4_o6MPR_gesamt.pdf

Rátai, B. (2005). Virtuális jelenlét és virtuális világok (Virtual presence and virtual worlds) In Dömölki, B., Kósa, Zs., Kömlödi, F. & Rátai, B. *Az információs társadalom technológiai távlatai. Tanulmány. (Technological prospects of the information society)* Nemzeti Hírközlési és Informatikai Tanács, 2005 szeptember. http://www.nhit-it3.hu/it3-cd/13.Virtualis_jelenlet_es_virtualis_vilagok.pdf

World Internet Project - Helyzetkép a magyar társadalomról 2007, kézirat. (World Internet Project - the Hungarian report) Also available in English: "Mapping the digital future" Hungarian society and the Internet. <http://www.tarki.hu/adatbank-h/kutjel/pdf/a717.pdf>

Section Editor: Pedro Verdelho

The legal section of the newsletter aims to describe and discuss the most relevant subjects both at the international and internal level specially in Europe, but also in Latin America, Asia and Africa, referring to the evolution of cybercrime and the new adopted legislations. All contribution provided by readers is welcome, by comments or by submitting articles for publication. If you have any legal issue to present, please contact the Editors.



RICARD MARTÍNEZ

Coordinator of the Study Area of the Spanish Data Protection Agency

EVIDENCE OF ILLEGAL CONDUCT IN DATABASES SUBJECT TO COMPLIANCE WITH HIGH-LEVEL SECURITY MEASURES IN SPANISH LEGISLATION *

The purpose of this paper is to highlight a peculiarity of Spanish data protection legislation that applies to the possibility of proving certain types of conduct. Indeed, in files with personal data subject to high-level security, there are security obligations that require the registration of every user's actions. Accordingly, the relevance of the case arises from the fact that the guarantee of the right to data protection when processing certain types of information includes the practical result of the obligation to guarantee the traceability of certain types of conduct. This makes it possible to obtain evidence of users' conduct.

The adoption of security measures described hereunder generates a twofold result. First of all, from a preventive point of view, the information system user is aware that his/her conduct will be registered and, therefore, should assess the consequences of the inappropriate manipulation of personal data. Secondly, if the conduct takes place and the data is accessed, manipulated or exported illegally, the conduct could be proved.

The interest or peculiarity of the Spanish system arises from the fact that this obligation is not the result of a technical security standard, but rather of a legislative requirement provided by Royal Decree 1720/2007, dated 21 December, which adopts the consolidating regulations of Organic Statute 15/1999, dated 13 December, on the Protection of Personal Data (hereinafter called RDLOPD). Therefore, if the party responsible for a file processes a certain type of data, he/she must necessarily include what is referred to as an "access register", as described hereunder.

1. Security levels

In Spain, the aforementioned regulations require that any file containing personal data must adopt security measures that are structured into various levels. Article 81 of the RDLOPD defines the security levels to be applied to files in accordance with the type of data they contain. The provision identifies three levels (basic, medium and high), for each of which it sets the measures that are to be adopted. Mention must be made of the fact that the different security levels are accumulative and, therefore, each level incorporates the measures provided for the level(s) immediately below it.

* Original article language: Spanish. The original article may be found at the following [link](#)

Author's note: the aim of this paper is limited to showing how the application of personal data protection legislation can contribute to the evidence of conduct in relation to files subject to the said legislation. I would like to acknowledge the invaluable collaboration of Elena Domínguez Peco, whose opinion on procedural issues has helped with the final draft of this document.





Article 81 RDLOPD is a complex provision and cases in which high-level security applies are justified in accordance with the entity of the legal right that is to be protected. With regard to the purpose of this paper, the adoption of high-level security measures is required in the following cases²:

- Files with data on ideology, union affiliation, religion, beliefs, racial origin, health and sex life
It is evident that these data, which coincide with the data given special protection by article 7 of Organic Statute 15/1999, dated 13 December, on the protection of personal data (hereinafter called LOPD) respond to the fact that they form part of the most intimate part of an individual's life and to the potential for discrimination that could result from their processing.
- Files that contain or refer to data collected for police purposes without the consent of the affected individuals.

The importance of protecting police data is obvious, but it does not arise exclusively from the need for protecting public safety and the appropriate development of police investigations. >From the citizen's point of view, consideration must be given to the fact that Spanish legislation contains a privileged system for the processing of such data. Accordingly, articles 22 to 24 LOPD contain exceptions to the duty to information and consent (including the processing of specially protected data) and to the principle of data quality and rights to access, correct and strike. In addition, this security requirement is also justified by the growing importance of computer tools in police work and their application to the future arrests of delinquents or potential delinquents, which can be easily verified, and the use of investigation files as potential registers of criminal records which, at least in terms of evidence, offer information about the danger of a certain individual.

- Files that contain data arising from acts of gender violence.

² Mention must be made of the exceptions:

- Files or data processing on ideology, union affiliation, religion, beliefs, racial origin, health and sex life when:
 - (a) The data are used for the sole purpose of transferring money to the institutions of which the affected parties are associates or members.
 - (b) Non-computerised processing or files in which the said data are stored by coincidence or in a subsidiary way and not related to the purpose thereof.
- The files or processing that contain data on health and refer exclusively to the level of disability or the mere declaration of the condition of disability or invalidity of the affected party for the fulfilment of public duties.
- The registration of accesses as defined in this article will not be necessary in the following cases:
 - (a) When the party responsible for the file or the processing is an individual.
 - (b) When the party responsible for the file or the processing guarantees that only he/she has access and processes the personal data related to the purpose thereof.
- The files or processing that contain data on health and refer exclusively to the level of disability or the mere declaration of the condition of disability or invalidity of the affected party for the fulfilment of public duties.
- The registration of accesses as defined in this article will not be necessary in the following cases:
 - (a) When the party responsible for the file or the processing is an individual.
 - (b) When the party responsible for the file or the processing guarantees that only he/she has access and processes the personal data.
- The files or processing that contain data on health and refer exclusively to the level of disability or the mere declaration of the condition of disability or invalidity of the affected party for the fulfilment of public duties.
- The registration of accesses as defined in this article will not be necessary in the following cases:
 - (a) When the party responsible for the file or the processing is an individual.
 - (b) When the party responsible for the file or the processing guarantees that only he/she has access and processes the personal data.



In the case of gender violence, besides the fact that the information systems that process these data can include information on the health of victims or aggressors, it is true that the guarantee of the security of this information is essential, since it concerns the life and physical integrity of the former.

- Finally, files whose responsibility corresponds to the operators that provide electronic communication services that are available to the public or operate public electronic communications networks in relation to traffic data and location data will be subject not only to basic- and medium-level security measures, but also to high-level security measures corresponding to the establishment of an access register.

The legislator refers to the files that have been generated by the said operators as a result of the adoption of Directive 2006/24/CE. This measure is justified by at least two types of reasons. First of all, they are data that offer relevant personal information from the point of view of personality profile. However, they also constitute information of police interest, as per the obligations applied to operators by Act 25/2007, dated 18 October, on the conservation of data related to electronic communications and public communications networks. Indeed, the said operators must keep the data generated or processed within the framework of the provision of electronic communication services or public communication networks. In addition, they must provide the said data to the authorised agents when so required by the corresponding judicial authorisation for the detection, investigation and trying of serious crimes as per the criminal code or special criminal legislation.

Therefore, it is a case of the protection of personal data that have a dual characteristic: they are data of police interest and also data that form part of the fundamental right to the secrecy of communications.

2. The access register

The access register is provided in article 103 of the RDLOPD and requires the adoption of security policies on various levels:

- At least the following must be saved from each access attempt: user ID, the date and time of the access, the file accessed, the kind of access and whether access was authorised or denied.
- If the access was authorised, the information that identifies the accessed record must be saved.

The main purpose of the access register is to avoid improper, fraudulent or incorrect access and, if the process for identifying and authenticating an authorised user is performed correctly, there is an exact record of when the access took place.

Another fundamental purpose of the access register is that "the type of access" is registered and "the information that identifies the register that is accessed" must be saved, where the minimum period for keeping the registered data is two years.

In practice, all this makes it possible to know whether the user accessed for query purposes or had the option and capacity for exporting, modifying or including data. Mention must be made of the fact that during its First Open Annual Session³, the Spanish Data Protection Agency stated that the said traceability should be understood in terms of past action. Therefore and by way of example only, if a user were to change a computerised medical record to alter a diagnosis or any other information, the register would consider that the register has been modified, but not the content of the modification. Accordingly, if an error were made comprising the exclusion in a patient's computerised records of his/her allergy to a certain drug and, subsequently, in order to hide the conduct to avoid claims for professional liability, the information were then included, the exact date, hour and minute when the user manipulated the data would be recorded.

Furthermore, there is a duty to regular and periodical control, since "the security manager⁴ will undertake to review the control information registered at least once a month and draw up a report on the reviews made and the problems found".

Another relevant and complementary matter arises from the fact that the access register is not an isolated measure, but rather should be understood in the context of use of each personal file or database. The data subject to protection cannot be accessible in the same way for each system user. Their level of knowledge and capacity for manipulation depends on their specific functional profile. In the Spanish system, this limitation, which responds to the most basic concept of common sense, has the rank of regulation and, in the case of personal data, is mandatory. Indeed, article 89 RDLOPD⁵, requires the documentation of the functional profiles of each user and article 91 RDLOPD⁶ limits the capacities of each user to those that correspond to his/her functional profile, providing the duty to prevent access to information that is not within his/her competency.

³ During the session, the following question was put forward:

"What should the scope of the access register be? What is its level of traceability regarding the information that identifies the register that is accessed in relation to the changes made?"

The information required to identify the register that is accessed must be saved, together with the modification thereof, but the scope should not affect the specific content thereof".

Available at https://www.agpd.es/portalweb/jornadas/1_sesion_abierta/index-ides-idphp.php#.

⁴ This is defined as follows:

"Security manager: Individual or individuals to whom the party responsible for the file has formally assigned the function of coordinating and controlling the applicable security measures".

⁵ This provides:

"Article 89. Functions and duties of personnel.

1. The functions and duties of each user or user profile with access to personal data and information systems will be clearly defined and documented in the security document".

⁶ This provides:

"Article 91. Access control.

1. Users shall only have access to the data and resources they may require for performing their functions.

2. The party responsible for the file will ensure that there is an updated list of users and user profiles and the accesses authorised for each one.

3. The party responsible for the file shall establish the necessary mechanisms that prevent a user from accessing resources that require rights other than those that are authorised.

4. Exclusively, the personnel thus authorised in the security document may grant, change or cancel the authorised access to resources in accordance with the criteria set forth by the party responsible for the file.

5. Personnel not employed by the party responsible for the file having access to resources must be subject to the same terms and conditions and duties to security as his/her own personnel".

However, this type of limitation may be inferred from other legislation. In the area of health, article 16 of Act 41/2002⁷, regulates the uses of medical records. The provision lays down criteria that require the differentiation of the functions of administrative personnel and health personnel, the differentiation of accesses by medical-care personnel, inspection personnel and data communications, and requires the development of procedures that record accesses to medical records⁸.

Similarly, in its recent Report 0318/2009, the Spanish Data Protection Agency, partly considering the above-mentioned arguments, states that in the case of access to administrative registers that provide support for judicial activities, only the officers that carry out the functions provided in articles 5, 6 and 7 of Royal Decree 95/2009, dated 6 February, which regulates the system for administrative registers for support for the Justice administration, can access the system and only in relation to the resources that are bound to their functions⁹.

Finally, mention must be made of the fact that this set of measures is also applied to the processing of personal data on non-computerised media. Accordingly, article 113 RDLOPD requires the establishment of access controls. First of all, access to the documentation will be limited exclusively to authorised personnel. In addition, it requires the establishment of "mechanisms that identify the accesses made if the documents can be used by more than one user". In addition, there must be a procedure in place for access by individuals who are not users authorised by the security document (such as external personnel (responsible for the processing), authorities in inspection processes, individuals authorised to consult the information, etc.) and for keeping a register of their accesses. Therefore, there is also traceability when the information system or part thereof is not computerised.

⁷ Act 41/2002, dated 14 November, the basic regulatory law on patient autonomy and rights and duties regarding medical information and documentation.

⁸ This provides:

"Article 16. Uses of medical records.

1. The medical record is an instrument fundamentally designed to guarantee appropriate patient care. The health care professionals at the centre that perform a diagnosis or treatment for the patient have access to the latter's medical record as a fundamental tool for providing the appropriate care.
2. Each centre must put in place the methods that enable access to each patient's medical record by the professionals looking after him/her at any time.
3. Access to the medical record for judicial, epidemiological, public health, investigation or educational purposes is governed by the provisions of Organic Statute 15/1999, on the protection of personal data, and the General Health Act 14/1986 and other legislation applicable in each case. Access to the medical record for these purposes requires the conservation of the patient's personal identification data separate from the medical-care data, so that general anonymity is guaranteed, unless the patient himself/herself has given his/her consent for the data not to be kept separately. This excludes the cases of investigations by judicial authorities where it is considered essential to unify the identification data with the medical-care data, where the decisions handed down by the judges and courts in the corresponding process will apply. Access to the data and documents of a medical record is strictly limited to the specific purposes of each case.
4. The administrative and management personnel of health centres may only access the medical record data related to their own functions.
5. The duly accredited health personnel that carry out inspection, assessment, accreditation and planning functions have access to medical records in fulfilment of their functions for verifying care quality, respect for the patient's rights and any other obligation that corresponds to the centre in relation to patients and users or the health administration itself.
6. The personnel that accesses medical record data as part of their functions are subject to the duty to secrecy.
7. The autonomous communities will regulate the procedure to ensure that there is a record of accesses to medical records and the use made thereof".

⁹ Report 0318/2009, on security measures for accessing administrative registers that support judicial activities. Available at https://www.agpd.es/portalweb/canaldocumentacion/informes_juridicos/medidas_seguridad/index-ides-idphp.php.



3. A practical case

In the recent decision of 11 February 2009, handed down by the Provincial Court of Majorca, it has been possible to verify the value as evidence of the establishment of functional profiles and the access register to which we have referred. Although it must be pointed out that the judge does not refer to the legislation on the protection of personal data regarding data security at any time, the case and the evidence brought show the effectiveness of the access register provided by the consolidating regulations of Organic Statute 15/1999.

The case was a crime of the revelation of secrets as per article 197 and following of the criminal code. The case refers to the access to the computerised medical record of a doctor by another doctor, who was a colleague at the same health centre.

The expert evidence came from the party responsible for the health care systems, who has the appropriate permission for accessing the system. Basically, the expert accredits, and they appear as facts declared proven by the sentence, the exact days and times at which the access took place and the route followed in the computer application to access the data. As pointed out above, the evidence only shows that certain data have been accessed and the identity of the reported doctor, but it is not capable of fully establishing in greater detail the complete action that took place for reasons that have to do with the operation of the system. Indeed, from what is stated in Legal Ground Five, it can be deduced that the information system does not record any material access to health data in the victim's medical records. This is not necessary if it is the result of the said access not having been actually made or the result of an application programming error that has caused the incorrect operation of the register. Indeed, if the system had complied with the requirements provided in the RDLOPD and there had been access to health data, it should appear.

4. Security levels, traceability and electronic evidence

As deduced from the legal argument of the above sentence, the fulfilment of high-level security measures as provided in Royal Decree 1720/2007 provide sufficient traceability of the actions taken by an information system user to provide sufficient evidence of illegal conduct. This is without prejudice to the valuation of the evidence in a hypothetical criminal process, in which the general rules that govern the validity of evidence obviously apply.

In this case, taking into consideration the computerised files, the evidence would be obtained using electronic mechanisms so that the conclusion can be drawn that, in this type of typical action, electronic evidence becomes an item of evidence of special interest for the process.





Accordingly, special mention must be made of the peculiarities of this type of evidence, since, unlike normal practice, it does not focus on finding the content or material aspect of the action (the specific files that were viewed and, where applicable, modified) but rather on the process, in other words, the fact that a file was accessed.

This peculiarity also affects the subjective nature of the evidence, since, as the personal data are not compromised, the request for the expert's intervention does not seem to require any reasoned judicial decision, but rather, as in the case above, the party reporting the access can require the intervention of experts in electronic evidence. It is true that, in the case we have used as a basis, the party responsible for the files, who has permission to access them, was required. The question that arises is what would jurisprudence say if this action were carried out by a company that specialises in obtaining electronic evidence?

Here again, the question is answered in legislation on data protection. The basis for the answer to the question is that the party responsible for the file in question is obliged to perform a monthly audit of the access register to which we refer, as well as to solve and document any security incidents. What happens if the said party resorts to a specialist company for the said order? Legislation on personal data protection provides the figure of data processing by third parties. In Spain, the LOPD requires the formalisation of a specific contract, as provided by article 12 thereof, to guarantee the provision of services under appropriate control conditions and guarantees¹⁰.

To conclude, the fulfilment of the high-level security measures provided by Royal Decree 1700/2007, dated 21 December, which adopts the consolidating regulations of Organic Statute 15/1999, dated 13 December, on the protection of personal data, has, in this case, enabled sufficient traceability of the actions of an information system user to provide sufficient evidence of illegal conduct.

¹⁰ This provides:

Article 12. Access to data by third parties.

1. The consideration of the communication of data shall not apply to the access by a third party to data when the said access is necessary for providing a service to the party responsible for the processing thereof.
2. The processing of data by third parties must be regulated by a contract in writing or in some other form that proves its existence and content. The contract must provide that the person processing the data shall only process the data in accordance with the instructions from the person responsible for the processing and that the said data shall not be used or applied for any purpose other than that which appears in the contract and it shall not be communicated to other persons, not even for the purpose of conserving the said data. The contract shall likewise stipulate the security measures referred to in article 9 of this Act, which the party responsible for processing is required to implement.
3. Once the contractual services have been provided, personal data shall be destroyed or returned to the person in charge of processing, as shall any other medium or documents that contain personal data that may be processed.
4. Should the party responsible for the processing use such data for other purposes, disclose them or otherwise use them in breach of the contract, the contractor shall also be deemed to be responsible for processing and will answer personally for any violations incurred in respect thereof.

Section Editor: Mrs. Elena Dominguez Peco

This section will expose the different realities regarding the data protection policies in different countries. You are welcome to collaborate in the development of the section or give us your opinion by contacting the Editor.





EDDY WILLEMS

Security Evangelist at Kaspersky Lab and EICAR
TECHNICAL COMPLEXITY IIIII

THE INCREASING PROBLEM OF DRIVE-BY DOWNLOADS

Eddy joined Kaspersky Lab in 2007, and is currently based in the Benelux region. He is involved in anti-malware and security research, and regularly speaks to the media, distributors, resellers and end users. He also acts as a contact for local law enforcement agencies. Eddy has a particular interest in educational projects designed to increase the security awareness of young users.

Before joining the company, Eddy worked as Anti-Malware Technology Expert for NOXS, a Westcon Group Company. Throughout his career he has been actively involved with security industry bodies, acting as a founder member and Director of Press and Information of EICAR and as a Wildlist reporter.

Unfortunately, the maturity and sophistication of the web has attracted the attention of well-organized malware purveyors who are now intent on using the Web to deliver their viruses, spyware, Trojans, bots, rootkits, and fake security software. The anti-virus industry refers to this covert downloading of malware, which occurs at Web sites without the user's awareness, as a "drive-by download." In this article, we will explore what actually happens during a drive-by attack, the lures used to perpetrate attacks, the technology behind the attacks, and the use of drive-by download attacks in personal data theft and computer takeovers.

Before we explore drive-by downloads in more detail, it is useful to understand how this type of attack has exploded in recent years. It is also helpful to understand that the same malware, and often is, delivered in different ways – sometimes by e-mail, sometimes by visiting a Web page, sometimes by other methods. Drive by malware delivery is of increased appeal to cybercriminals simply because it is, in general, a more stealthy form of infection that results in more successful attacks. According to more recent data from ScanSafe 74 percent of all malware spotted in the third quarter of 2008 came from visits to compromised Web sites. Let's explain now how the attacks work, the techniques used to lure targets to rigged Web sites, the sophisticated exploit kits and the applications they target, the complicated maze of Web redirects, and the payloads used to conduct identity theft and computer takeover attacks.

*Technical complexity rating shows the technological experience level needed to easily understand the article contents. Level for this interview is MEDIUM IIIII.

Browser Attacks

To fully understand the dramatic shift to using the Web browser as the attack tool, it is useful to revisit the history of major Internet-based computer attacks. During the “Internet worm era,” when attacks like Code Red, Blaster, Slammer and Sasser wreaked havoc on corporate networks, hackers used remote exploits against Windows operating system vulnerabilities. (A remote exploit is one in which the malware resides on a network-connected server, exploits legitimate code on the user’s computer, but doesn’t require prior access to the user’s computer to exploit the vulnerability in the code.) Malicious executables, such as Melissa, were also attached to e-mail or they arrived via instant messaging or peer-to-peer applications.

Microsoft reacted to the worm attacks in a positive way. They added a firewall, which is turned on by default in Windows XP SP2, and implemented several anti-worm mitigation mechanisms in the operating system. With automatic updates enabled on Windows, end users got some assistance with regularly applying operating system patches. Businesses and consumers also got smarter about blocking attachments or not clicking on strange executables. Both factors forced attackers to shift tactics, moving up the stack to target third-party applications and to perfect the art of social engineering.

This evolution also drove the emergence of a stealthy new technique – the drive-by download – that uses the browser as the mechanism to connect computer users to servers rigged with malicious exploits. In the drive-by attack, the malicious program is automatically downloaded to your computer without your consent or even your knowledge. The attack actually occurs in two steps. The user surfs to a Web site that has been rigged with code that in turn redirects the connection to a malicious third-party server hosting exploits. Figure 1 shows the basic structure of a drive-by download attack. These exploits can target vulnerabilities in the Web browser, an unpatched browser plug-in, a vulnerable ActiveX control, or any other third party software flaws.

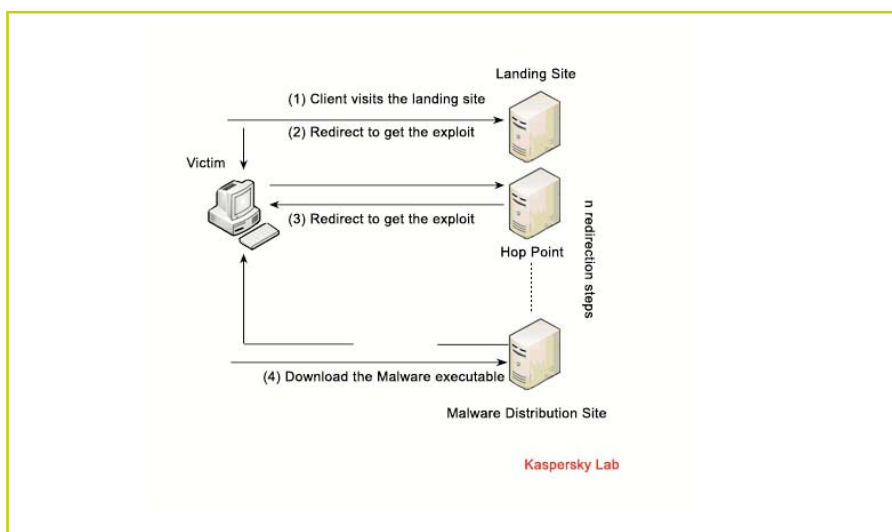


Figure 1 - Structure of a Drive-by Download Attack



As the figure indicates, there may be any number of redirections to different sites before the exploit is actually downloaded. According to data from Kaspersky Lab and others in the security industry, we are in the midst of a large-scale drive-by download epidemic. Over a recent ten-month period, the Google Anti-Malware Team crawled billions of pages on the Web in search of malicious activity and found more than three million URLs initiating drive-by malware downloads. In the early days of drive-by downloads, attackers typically created malicious sites and used social engineering lures to attract visitors. This continues to be a major source of malicious activity online, but more recently hackers have compromised legitimate Web sites and either secretly exploit script or planted redirect code that silently launches attacks via the browser.

Exploits, exploits and exploits

One high-profile Web site compromise in 2007 provides a glimpse at how drive-by downloads are launched against computer users. In the weeks leading up to the NFL Superbowl game, Miami's Dolphin Stadium site was hacked and rigged with a snippet of JavaScript code. A visitor to that site with an unpatched Windows machine was silently connected to a remote third party that attempted to exploit known vulnerabilities described by Microsoft's MS06-014 and MS07-004 security bulletins. If an exploit was successful, a Trojan was silently installed that gave the attacker full access to the compromised computer. The attacker could later take advantage of the compromised computer in order to steal confidential information or to launch DoS attacks. Later in 2007, the high-traffic "Bank of India" Web site was hijacked by hackers in a sophisticated attack that used multiple redirects to send Windows users to a server hosting an e-mail worm file, two stealth rootkits, two Trojan downloaders, and three backdoor Trojans. These are just two examples to highlight the extent of the problem on legitimate Web sites. In its tracking of Web-based malware threats, ScanSafe reported that by the middle of 2008, the majority of malware was being found on legitimate sites.

Malware exploit kits serve as the engine for drive-by downloads. These kits are professionally written software components that can be hosted on a server with a database backend. The kits, which are sold on underground hacker sites, are fitted with exploits for vulnerabilities in a range of widely deployed desktop applications, including Apple's QuickTime media player, Adobe Flash Player, Adobe Reader, RealNetworks' RealPlayer, and WinZip. Browser-specific exploits have also been used, targeting Microsoft's Internet Explorer, Mozilla's Firefox, Apple Safari, and Opera. Several targeted exploit kits are fitted only with attack code for Adobe PDF vulnerabilities or known flaws in ActiveX controls. Identity thieves and other malware authors purchase exploit kits and deploy them on a malicious server. Code to redirect traffic to that malicious server is then embedded on Web sites, and lures to those sites are spammed via e-mail or bulletin boards.

An exploit kit server can use HTTP request headers from a browser visit to determine the visitor's browser type and version as well as the underlying operating system. Once the target operating system is fingerprinted, the exploit kit can determine which exploits to fire.

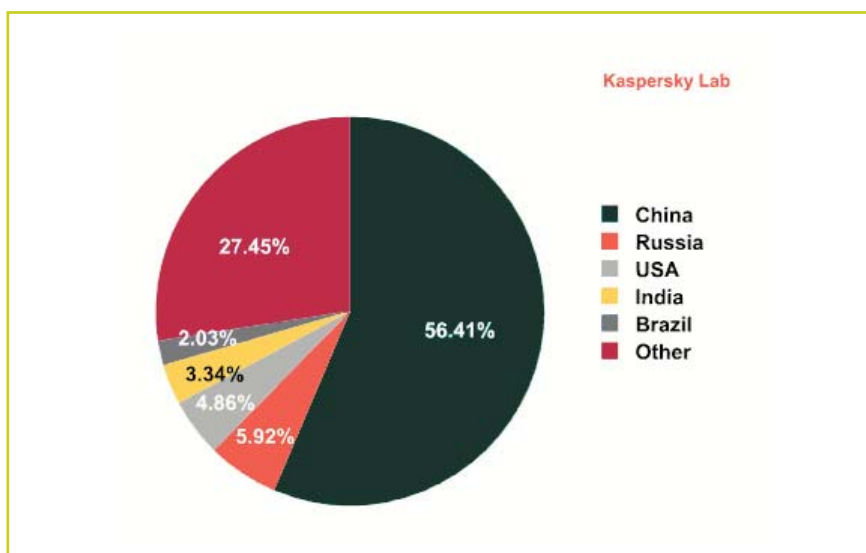
In some cases, several exploits can be sent at the same time, attempting to compromise a machine via third-party application vulnerabilities. Some of the more sophisticated exploit kits are well maintained and updated with software exploits on a monthly basis. The kits come with a well-designed user interface that stores detailed data about successful attacks. The data can range from operating system versions exploited, the target's country of origin, which exploit was used, and the efficiency of exploits based on traffic to the malicious site.

The real problem: patching your systems...

The drive-by download epidemic is largely attributed to the unpatched state of the Windows ecosystem. With very few exceptions, the exploits in circulation target software vulnerabilities that are known – and for which patches are available. However, for a variety of reasons, end users are slow to apply the necessary software fixes. Microsoft's Automatic Updates mechanism offers end users a valuable way to keep operating system vulnerabilities patched, but the same cannot be said for third-party desktop applications. Secunia, a company that tracks software vulnerabilities, estimates that about one-third of all deployed desktop applications are vulnerable to a known (patched) security issue.

Which countries

The following table shows the countries which rank most highly in terms of attempts to infect computers via the web.





Some solutions

It is important to note that most modern Web browsers – including Internet Explorer, Firefox, and Opera – have added anti-malware blockers that provide early-warning systems when users attempt to surf to a rigged Web site. These blockers provide good value but, because they are blacklist-based, they do not provide 100 percent protection to Web surfers. The most practical approach to defending against drive-by downloads is to pay close attention to the patch management component of defense. Let's try to sum up the most important solutions:

- Use a patch management solution that assists with finding – and fixing – all third party desktop applications. Secunia offers two tools – Personal Software Inspector and Network Security Inspector – that can help identify unpatched applications.
- Use a desktop browser that includes anti-phishing and anti-malware blockers. Microsoft's Internet Explorer, Mozilla Firefox, and Opera all provide security features to block malicious sites.
- Enable a firewall and apply all Microsoft operating system updates. Avoid using pirated software which has its updates disabled through WGA.
- Install anti-virus/anti-malware software and be sure to keep its databases updated. Make sure your anti-virus provider is using a browser traffic scanner to help pinpoint potential problems from drive-by downloads.
- Try to browse in a virtual environment and quit to return to a safe snapshot from the clean situation before, this method can help to avoid the possible new attacks. This method can be done by use of a virtual environment or some AV vendor package functionality. For instance Kaspersky lab is calling this the Green Zone. This application can even roll back all the system changes made by an application.

These steps toward managing the vulnerabilities continue to offer the greatest, most valuable protection against drive-by download attacks.

However it's not over yet ... Recently there has been a clear trend for cybercriminals to use a range of sophisticated drive-by downloads to install malware on victim machines. Overall, cybercriminals are becoming increasingly Web-oriented. This makes it particularly important for users to update their operating systems and application software regularly and to keep their antivirus solutions up-to-date. I hope we all can stay safe for the next wave of drive-by downloads by using these solutions.

Note of the Author: Thanks to Ryan Naraine in helping me out with this article

Section Editor: Matías Bevilacqua

This section will focus on the technical side of cybercrime and electronic evidence. The reader is highly encouraged to contribute to this section. Given the technical complexity rating system used, we are open to divulgative introduction articles on technology, state-of-the-art white papers and everything in between. Please contact the Editor if you'd like to contribute to this section.





BERNHARD OTUPAL

Assistant Director of INTERPOL's Financial and High Tech Crime Sub-Directorate

THREATS OF CYBERCRIME AND INTERPOL'S RESPONSE

Bernhard Otupal is the Assistant Director of INTERPOL's Financial and High Tech Crime Sub-Directorate based at the General Secretariat headquarters in Lyon, France where he oversees INTERPOL's activities in the fields of financial crime, high tech crime, counterfeit currency and credit cards and intellectual property rights violations. He holds a Master of Science degree in Forensic Computing and Cyber Crime Investigations of the University College, Dublin where he became an adjunct Senior Lecturer in January 2009.

Mr Otupal began his career as a police officer in 1984 with the Gendarmerie in Upper Austria. In 1987 he became a detective for scene of crime investigations and in 1990 joined a local unit dealing with car theft investigations.

In 1993, Mr Otupal moved to Vienna to work in the Federal Ministry of Interior in the National Organized Crime Unit and subsequently in the same year to the National Counter Terrorism Unit.

In 1998, he created a Central National Computer and Network Crime Investigation Unit and since August 1999 worked there as the Head of Section responsible for national and international cooperation and co-ordination of IT related investigations. Since then, Mr Otupal has represented Austria at the United Nations (UN), Council of Europe (COE), Europol, the Organization for Security and Co-operation in Europe (OSCE) and several other international organizations.

Mr Otupal was responsible for setting up national training programs and in 1999 he became the permanent Austrian representative to the European Working Party on IT crime and in this capacity, a member of the INTERPOL Cyber Crime Training Group.

Mr Otupal is a frequent consultant and trainer around the globe on topics related to high tech crime, psychological aspects related to the Internet and international aspects of law enforcement. He was also a Lecturer at the University College of Hagenberg/Upper Austria of Computer and Media Security, and has authored several publications on IT Crime and suicidal activities in connection with the Internet.



ENAC: Would you please give us a short insight into the role of INTERPOL and the impact it has on the efforts of police in different countries to combat cybercrime?

Bernhard Otupal (BO): The world's largest international police organization, INTERPOL, facilitates cross-border police co-operation among its 187 member countries. Central to all INTERPOL's activities is I-24/7, the Organization's global police communications network which enables police around the world to exchange information securely and to access vital databases in real time. INTERPOL uses a system of colour-coded international notices to locate, arrest or provide warnings about fugitives and other criminals and can also be used to distribute information about new modus operandi and early alert messages. The I-24/7 network currently connects National Central Bureaus (NCBs) in all member countries and it is planned to extend direct access to all available cybercrime units, making INTERPOL's IT Crime Manual instantly available to them.

The INTERPOL Command and Co-ordination Centre at the General Secretariat headquarters in Lyon, France, provides a 24/7 service in all four of the Organization's official languages - Arabic, English, French and Spanish - for immediate response to enquiries from NCBs around the world. The Command and Control Centre (CCC) is also extending a network of contact points to major IT service providers for quick response in case of emergency.

Based within the Specialized Crimes and Analysis Directorate, the Financial and High Tech Crime Sub-Directorate has highly qualified police specialists available. The unit has also established a network of National Central Reference Points on IT Crime - currently 122 countries - for immediate response.

Also, each INTERPOL region has set up a Working Party on IT Crime which reacts to regional problems, provides training courses and develops recommendations for combating upcoming problems.

ENAC: What are the next cyber threats due to rapid changes in technology?

BO: With the project 'Fibre for Africa' a whole continent will have high speed connectivity in the very near future. Africa will be connected by the most up-to-date fibre optic technology. A network of inland backbones is also under construction at the moment. This project and others, like One Laptop Per Child will open up huge opportunities for development.

However this type of expansion also opens opportunities for the criminal abuse of these technologies. Legislation has to be brought up to date in many countries and police trained not only in the use of these new technologies, but also in how to protect citizens and conduct specialist investigations. A second problem is the current economic situation. Experts fear that as many high qualified IT-technicians lose their jobs worldwide, some of them might be recruited into organized crime networks and cause additional economic damage.

In general, criminal activities on the INTERNET have become highly organized over the past few years: a whole underground economy has been developed and is working very professionally to generate substantial profits.



ENAC: Are these countries prepared for these new threats and how can INTERPOL help them?

BO: Most of the developing countries, and here I mean developing in the sense of new technologies, make the mistake of seeing only the positive side of new economic possibilities such as new business models, or high speed connections. In many of these countries no up-to-date legislation is in place to tackle the upcoming problems. Police in many countries are neither aware nor prepared to deal with these modern technologies. Even worse these technologies are not available for police work itself.

INTERPOL identified this problem early on and is launching, together with private industry and academia, a number of initiatives in response to the problem.

For example INTERPOL is working very closely with the Council of Europe to introduce the Budapest Convention on Cybercrime to its member countries as a legislative framework. At the INTERPOL General Secretariat a system of Incident Response Teams has been set up to provide emergency assistance to countries that for the moment do not have sufficient resources or capabilities of their own. INTERPOL's Regional Bureaus will be equipped and trained to help directly in the regions, not only through forensic examinations, but also training. Training courses, based on the European AGIS programme are and will be provided in the regions as train-the-trainer programmes. At the moment, a new guideline for first responders, based on a document developed by the Australian Federal Police (AFP), is being produced and will be made available to police globally.

Together with the University College Dublin, the INTERPOL General Secretariat is developing several affordable tools for law enforcement which will soon be tested. Private industry has indicated its willingness to cover some of the production costs.

ENAC: What are the most prevalent type of technology related crimes the world is facing?

BO: In recent years the fastest growing type of criminal technologies are BotNets. These robot networks consist of thousands, up to millions of infected computers which are controlled remotely by criminals through complex systems that are very difficult to investigate. These huge numbers of computers can be abused for a wide range of criminal activities such as distributed denial of service (DDoS) attacks, black mailing or spam; they can be used to hide terrorist material or child pornography. These BotNets no longer need to be set up by criminals, since they are made available for sale by organized crime organisations. The problem is, the owners of infected machines don't know that their computers are abused for criminal activities.

Another fast growing problem is that of virtual worlds. These worlds are abused by criminal and terrorist organizations for recruitment, money laundering, training and propaganda. Policing these worlds is very difficult and often issues in the virtual worlds are transferred to the real world. Activities in these virtual worlds have led to murder, divorces, theft and child abuse.

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008





ENAC: What is INTERPOL doing to keep its capability to combat these types of crime up to date?

BO: INTERPOL has a global network of highly skilled experts available. They see problems popping up immediately and develop countermeasures. Under the umbrella of the INTERPOL Global Security Initiative (GSI) a new cyber initiative has been developed and is currently being implemented. It includes five focus areas:

- 1: Forensic capacity for incident response
- 2: Training and development
- 3: Computer crime situational awareness (newsletter, early warning, notices)
- 4: Private public partnership
- 5: Research of new technologies

All this will happen in close co-operation with other organizations and bodies like International Multilateral Partnership Against Cyber Threats (IMPACT), International Organisation on Computer Evidence (IOCE), High Tech Crime Investigators Association (HTCIA), Cybercrime Centre of Excellence Network for Training, Research and Education (2Centre), but also academia and the private industry. INTERPOL will also continue its efforts to support projects of other organizations such as the European Union.

ENAC: Using your crystal ball, give us an insight into what the global LE capability will consist of in 10 years time.

BO: Looking at the rapid development of the Internet and the criminal abuse possibilities it offers, an international approach has to be the answer from the law enforcement side.

Today, most police are working only within their geographical and legislative boundaries; this needs to change quickly. International laws need to be established and international investigations have to be enabled. Private industry will have to take over some parts of police work, for example, collecting evidence, and police have to adopt industry practices such as administrating "whois" domain name information. Victim protection has to become more important than data protection, which these days mainly protect the criminals, since the average citizen has nothing to hide.

International centre's of excellence for policing the Internet have to be established in order to help those, who don't yet have their own capability. These areas have already been identified and are misused by criminals. The problem is that they use these safe havens to run global attacks. So it is of global interest to help these countries and their police forces.

Section Editor: Mr. Nigel Jones

This section of the newsletter aims to provide the most up to date international information relating to law enforcement in the cybercrime and IT forensics fields. This will only succeed if people are willing to contribute articles of interest. We recognise that investigations involve sensitive techniques and do not expect detailed information to be disclosed. It may be of interest and benefit to our readers to hear of specific challenges, especially where they impact across borders. If you have any area of interest that you may be willing to write an article about or be interviewed for publication, please contact the law enforcement section Editor to discuss how your information may be made available for the wider efforts to counter cybercrime.



RAOUL CHIESA

Cybercrime Issues & Strategically-Related Alliances -
Technical contact at UNICRI



unicri
advancing security, serving justice,
building peace

UNITED NATIONS & UNICRI IN FIGHT AGAINST CYBERCRIME

Raoul Chiesa was born in Turin on 3rd July 1973: he has been one of the first hackers in Italy. His first wanderings on the international computer networks of the biggest Eighties and Nineties companies date back to 1986, when he was 13, under the nickname of Nobody. After a series of sensational interferences, such as telcos and other military, governmental, and financial institutions, he was officially recognised as one of the main members of the European and North American hacker scene by international authorities in 1995.

As founder and C.T.O. of @ Mediaservice.net, an Italian based vendor-independent, security consulting firm working all around EU, Middle and Far East, Raoul Chiesa has been active in the field of computer security research at a high level since 1997, together with a team of experts and technicians who gave their contribution to national and international Security R&D projects.

Since 2003, Raoul Chiesa is the Southern Europe and Northern Africa referent for TSTF (Telecom Security Task Force), an international panel of consultants with high level skills on telcos present in four continents; in the same year Raoul Chiesa was elected in the ISECOM's International Executive Board, following his role of Director of Communications for the Institute (2004); Raoul belongs also to CLUSIT (Italian Computer Security Association) and OWASP Italian Chapter (Open Web Applications Security Project) Boards of Directors, and he's a member at ICANN and APWG (Anti-Phishing Working Group).

Since 2005, he's a consultant at UNICRI on cybercrime issues. Raoul authored and co-authored various books and papers related to ICT Security and Hacking.

United Nations (further UN) is probably the most known international organization. It was established in 1945, and since then it is trying to achieve world peace and is playing significant role in international security, economic development, social progress, human rights, and international law. The logo of the institution is: United Nations - It's your world! We have asked Raoul Chiesa from UNICRI if only physical space is included in this logo or also peace and security in cyberspace is important for UN.





ENAC: The UN logo states "United Nations - It's your world!" You co-operate with UNICRI, a UN Research Institute. What's UNICRI's payoff in its logo?

Raoul Chiesa (RC): Well, in UNICRI's logo you will find the following:

"Advancing security, serving justice, building peace".

I really think that the above resumes very well our mission.

In fact, the United Nations Interregional Crime and Justice Research Institute - UNICRI - was created in 1968 to assist intergovernmental, governmental and non-governmental organizations in formulating and implementing improved policies in the field of crime prevention and criminal justice.

UNICRI sees itself as 'the first response broker.' We become known for our dynamic, fresh and innovative approach in applied research.

UNICRI's activities tackle major concerns in the field of crime prevention and criminal justice, such as corruption, security governance and counter-terrorism, organized crime.

Other areas of intervention are inter alia counterfeiting, environmental crime and cybercrimes, where we are focusing on right now.

Last but not least, protection of victims and cultural heritage is our important task. UNICRI also conducts major programs in criminal justice reform, with a special focus on juvenile justice.

ENAC: Please describe in few words your position and main tasks within UNICRI.

RC: Right now I'm a consultant on cybercrime issues. I'm taking care of international strategic alliances, from a very-technical point of view. This means, e.g., relationships with CERTs and specialized Computer Crime Units, as well as private and public companies co-operating with UNICRI on this specific topic. I often attend IT Security events all over the world as a speaker, showcasing UNICRI and its activities, building our specialized-contacts network. Also, I work with my colleagues on ICT crime-related projects, that can be found on http://www.unicri.it/www/cyber_crime/index.php

ENAC: How important is fight against cybercrime for UNICRI? Do you think this type of crime is a serious threat to whole global community or is it affecting only more technological developed countries?

RC: We are talking about a crime category that is rising up continuously, while affecting the global community: children and families, standard IT users, professionals, SMEs and multinationals, governments and military environments. This obviously means that fighting cybercrime is among our top priorities.

ENAC: How is UN involved in fight against cybercrime? What actions do you take to combat this type of crime? Are there any special projects or programmes opened for the fight against cybercrime?

RC: Right now we are working on different research areas: fighting digital paedophilia, training LEAs on

digital forensics, profiling hackers (HPP - Hackers Profiling Project), analyzing the Spam phenomenon with new, different and innovative views, and CNI's (Critical National Infrastructures) and SCADA (industrial automation) security issues.

ENAC: What is the main or final goal UN would like to reach with the activities against cybercrime?

RC: ...Being able to act as a facilitator, allowing PPP focusing on these topics, supporting them with our worldwide network, vision, approaches and knowledge. Showing the right path, publishing research papers, experiences, useful info and tips, also for the end-user.

ENAC: Are there any special projects or programmes planned in the future to combat cybercrime?

RC: Yes, there are! We are writing down our new training programs for LEAs, Public Prosecutors and Lawyers. We will focus on open source, since many emerging countries could not fit the budgets needed for commercial products.

ENAC: Does UN cooperate with other institutions in the field of fight against cybercrime?

RC: Yes, we have very strong relationships and shared projects, especially with ITU and CYBEX. We are on the way to establish a wonderful research program - that

Section Editor: Liljana Selinsek

The reader is invited to contact the Editor to present his or her Institution's activities in reference to the fight against cybercrime, or any other contribution regarding this topic.





Country: Greece

Case citation: 1327/2001 - Payment Order

Name and level of Court: Court of first Instance of Athens

Keywords: Meaning of electronic document - evidential weight - private (manuscript) document - e-mail address as electronic signature

• SUMMARY

Between January 1999 and February 2000, the applicant company assisted the correspondent company with lodging arrangements made in Prague, Czech Republic, for groups of Greek tourists that visited Prague and were sent by the correspondent company, in furtherance of a service agreement that was orally concluded between the two companies in Prague. An authorized representative of the correspondent company sent an e-mail to the applicant, in which a debt of 42,760 DM was acknowledged, with a promise to pay the amount due before 15 August 2000. A second e-mail confirmed the intention to pay the debt and repeated the same promise as in the first e-mail.

The judge determined that the e-mails were legally delivered to the applicant and constituted private documents, and therefore provided full evidence, as defined in article 448 paragraph 2 of the Greek Civil Procedure Code. In the sending of a message by way of e-mail, the sender's will is identified with his electronic address, which has the characteristics of a manuscript signature, and was also a form of electronic signature. The attested copy of an e-mail, which exists in the receiver's hard disc, was determined to be a full proof that its contents come from its editor-sender, according to the provisions of article 445 of the Civil Procedure Code. The defectiveness of a message that has been sent directly refers to the traditional act of forgery in the physical world. The burden of proof lies to whoever appeals that defectiveness. The payment order for a debt that comes from an agreement that was concluded by way of e-mail was granted. The electronic message did not need to be authenticated by the Revenue Department.

For a translation of the case into English with a commentary by Michael G. Rachavelias, see *Digital Evidence and Electronic Signature Law Review*, 3 (2006) 104 - 107



Country: China

Parties: Yang Chunming v Han Ying

Case citation: Hai min chu zi NO.4670

Name and level of Court: Beijing Hai Dian District People's Court

Date of judgment: 14 July 2005

Keywords: Text messages - mobile telephone - loans of money - whether text messages evidence of loan - signature at end of message - whether electronic signature

• SUMMARY

In 2004, by a series of text messages between mobile telephones, the defendant requested, and the claimant agreed to lend a total of RMB 11,000 to the defendant. The money was remitted to the plaintiff by the claimant. The money was not repaid.

During the first hearing of the trial, the defendant acknowledged that the telephone number in question was used by her from July or August 2004 to the date of the hearing. However, during the second hearing, the defendant denied that she had used the telephone number. There was no evidence to show that the acknowledgement was made under oppression or gross misunderstanding by the defendant, and this led the court to believe that the telephone number was used by the defendant. The contents of the messages conformed to the amount and time recorded in personal business vouchers of the Industrial & Commercial Bank of China, and the contents of the messages in the mobile telephone illustrated the plaintiff's intention to pay the loan back. This led the court to accept that the money was borrowed.

The court also decided, in considering the Electronic Signature Law of the People's Republic of China, that messages stored in a mobile telephone conform to the form of an electronic signature and the data message, which meant that messages stored in a mobile telephone can give effective expression to the contents carried, and can readily be referred to; the addressees and recipients of the messages in a mobile telephone and the time of their dispatch and receipt can be identified. By examining the reliability of generating, storing and transmitting the data messages, the reliability of the methods used to maintain the completeness of the contents and the reliability of the methods for distinguishing the addressees of the messages of the messages in the mobile telephone provided by the claimant, the court concluded that the contents of the messages were true as evidence.

For a translation of the case into English with a commentary by Jihong Chen, see *Digital Evidence and Electronic Signature Law Review*, 5 (2008) 103 - 105



Country: Belgium
Case citation: CSWARE bvba v Pepijn Descampes, trader
Name and level of Court: Ghent Court of Appeal, Chamber 7bis
Date of decision: 10 March 2008

Keywords: E-mail - evidential value and force - electronic signature

• SUMMARY

Mr Descamps acted as a consultant to CSWARE. When CSWARE stopped paying for his services, Mr Descamps demanded the payment of ten outstanding invoices and bills. CSWARE claimed that both parties agreed in October 2003 that CSWARE would only accept invoices that had been approved by it in advance. CSWARE stated it informed Mr Descamps of this by e-mail and also claimed it objected to every invoice dated after October 2003. To prove its claims, CSWARE presented printouts of the relevant e-mails to the court. Mr Descamps, however, argued he never received any of the e-mails, and pointed out that the e-mails could easily have been produced after the event by anyone with sufficient technical knowledge.

The Court of First Instance appointed an expert to determine the true nature of the contested e-mails. The expert found that CSWARE used an internal e-mail system that did not route internal e-mails over the public internet. Consequently, internal e-mails never passed the servers of an independent internet service provider and never left a reliable audit trail. Moreover, CSWARE administered the e-mail server itself, and therefore had access to the mailboxes of all users. This system setup enabled CSWARE, in its capacity of system administrator, to manipulate the clock of the server and to send out e-mails with forged dates, possibly even under another name, should it wish to. Taking into account the architecture of the internal e-mail system and the possibility of manipulation, the expert stated there was no certainty as to whether or not Mr Descamps did in fact receive and read the alleged e-mails regarding the prior approval of invoices.

The Court of First Instance followed the reasoning of the expert and ruled in favour of Mr Descamps. CSWARE appealed on the grounds that the alleged manipulation of the e-mails was never proved, and that their evidential value would thus still stand. The Court of Appeal confirmed that the burden of proof was with CSWARE, and that CSWARE needed to prove it did in fact send the e-mails. The Court of Appeal did not accept the print-outs of the e-mails as evidence, also taking into account the fact that a colleague of Mr Descamps never received similar e-mails purportedly sent by CSWARE. Furthermore, some invoices and bills from the period October 2003 - January 2004 had been paid by CSWARE, even though no order forms had been issued and signed previously. The Court also noted that CSWARE never mentioned the e-mails until after it received the summons. The Court of Appeal therefore confirmed the decision of the Court of First Instance.

For a translation and commentary of this case into English by Patrick Van Eecke and Elisabeth Verbrugge, see *Digital Evidence and Electronic Signature Law Review*, 5 (2008) 98 - 102.



Country: Sri Lanka

Case citation: Marine Star (Pvt) Ltd v Amanda Foods Lanka (Pvt) Ltd

Name and level of Court: High Court of the Western Province

Case number: H. C. (Civil) 181/2007(MR)

Keywords: Short messages (SMS) - photocopy of SMS - admissibility

• SUMMARY

The plaintiff sought to adduce SMS messages into evidence by means of a photocopy of the SMS messages received on the screen of a mobile telephone. The photocopy of the SMS messages is secondary evidence. Unless the original digital text of the SMS is admissible into evidence, then the photocopy would not be regarded as evidence. The primary issue was whether the message received on the screen of a telephone was a 'document'.

The learned judge referred to the case of *Benwell v Republic of Sri Lanka*, 1979 (2) SLR 194, in which Collin Thorne indicated that 'Computer evidence is in a category of its own. It is neither original evidence nor derivative evidence and in admitting such a document, a court must be satisfied that the document has not been tampered with'. The learned judge, K. T. Chitrasiri, HCJ, sought to distinguish this decision by indicating that the SMS messages in question were not generated by a computer. The SMS messages could be admitted into evidence.

Procedurally, the Evidence (Special Provisions) Act No 14 of 1995 provide that evidence in respect of contemporaneous recordings and computer print-outs can be admitted into evidence, providing that a copy is given to the other party 45 days before the date fixed for trial, and the machine from which the copy was made is available for inspection by the other party. This procedure was not followed, which meant the court refused to allow the SMS messages to be admitted under the provisions of the Evidence (Special Provisions) Act.

The learned judge also considered the provisions of the Electronic Transactions Act No 19 of 2006, and considered the SMS messages to come within the meaning of a 'data message' under section 26, and therefore admitted the messages under section 21.

Source: Jayantha Jayasuriya, Deputy Solicitor-General, Attorney-General's Department, Sri Lanka

Section Editor: Mr. Stephen Mason

The reader is invited to send details of cases (both civil and criminal, reported and not reported) that have relevance to digital evidence direct to the Editor. Please provide the correct citation as it would be in your own country, together with a full copy of the judgment. Translations into English will be appreciated if it is possible. Also, if there are any significant items of legislation that are of interest, please inform the Editor of any such changes. It is important to understand that because digital evidence moves over physical borders with ease, the changes to national legislation dealing with digital evidence and cyber crimes affects all other nation states.



• CONFERENCES

1-2 September 2009

CFET 2009 3rd International Conference on Cybercrime Forensics Education & Training

Canterbury Christ Church University, Canterbury, UK

Purpose: A broad inclusive approach taken with respect to anything to do with the development of cybercrime forensics as a new discipline.

Web site: <http://www.canterbury.ac.uk/social-applied-sciences/computing/conferences/CFET2009/BCSCybercrimeForensicsSG.aspx>

15-17 September 2009

IMF 2009 5th International Conference on IT Security Incident Management & IT Forensics

Stuttgart, Germany

Purpose: IMF's intent is to gather experts from throughout the world in order to present and discuss recent technical and methodical advances in the fields of IT security incident response and management and IT forensics. The conference provides a platform for collaboration and exchange of ideas between industry, academia, law-enforcement and other government bodies.

Web site: <http://www1.gi-ev.de/fachbereiche/sicherheit/fg/sidar/imf/imf2009/>

17-18 September 2009

Internet Security Operations and Intelligence 7 (ISOI7)

San Diego, California, United States of America

Purpose: The main topics of interest are Internet infrastructure defense, cyber crime, online fraud, phishing, DDoS and botnets. ISOI is a closed conference for members of the different Internet security operations communities, bringing different groups together.

Web site: <http://isotf.org/isoi7.html>

13-14 October 2009

VII seminar on electronic evidence

Hesperia Hotel, Paseo de la Castellana nº 57, 28046 Madrid, Spain

Purpose: Cybex and the General Council of the General Council of Judicial Power have organized the annual seminar on electronic evidence. This seminar is aimed at judges, prosecutors, lawyers, members of judicial and governmental institutions and corporate members of legal, audit, security and personnel departments.

Web site: <http://www.cybex.es>





26-28 October 2009

Techno Forensics & Digital Investigations Conference

National Institute of Standards and Technology, Gaithersburg, Maryland, USA

Purpose: The Techno Forensics & Digital Investigations Conference is founded on the principles of standardization in the field of digital evidence investigation. The conference will cover many of the general disciplines in the areas of digital evidence investigation to include some of the latest information on software and hardware solutions.

Web site: <http://www.techsec.com/html/TechnoForensics2009.html>

13 November 2009

First International Workshop on Data Mining for Fraud Detection (DMFD) 2009

Chicago, United States of America

Purpose: Most if not all organizations have operational data that can be studied to reveal insights into fraudulent activity. This organizational data is commonly high volume, heterogeneous, multi-dimensional, distributed, and dynamic over time. Of particular interest to this workshop are data mining techniques that can be applied to organizational data to reveal fraudulent activity. Data mining focuses on algorithms to accurately detect patterns or specific instances in high-dimension data. This is the first workshop forum to specifically focus on this topic.

Web site: <https://sites.google.com/site/dmfd09/>

• LEGAL TRAINING

14-17 September 2009

European Certificate on the fight against Cybercrime and Electronic Evidence (ECCE)

Cyprus

Web site: <http://www.lexact.com.cy> and <http://www.cybex.es/ecce/en/>

26-29 October 2009

European Certificate on the fight against Cybercrime and Electronic Evidence (ECCE)

Italy

Web site: <http://www.teutas.it> and <http://www.cybex.es/ecce/en/>





- TRAINING OF LAW ENFORCEMENT OFFICERS

7-11 September 2009

ISEC cybercrime training programme – Forensic Scripting using BASH Course

Centro de Convenciones Mapfre, Avda. General Perón, 40 – 28020 Madrid, Spain

Purpose: This training course is part of the EC funded ISEC cybercrime training project. All travel, accommodation and subsistence costs are paid for by the project. Places are still available to law enforcement staff from the following countries: Bulgaria, Czech Republic, Estonia, Finland, Greece, Luxembourg, Poland, Slovakia, Slovenia, Sweden, Turkey and the Former Yugoslav Republic of Macedonia.

Anyone interested in these courses is asked to contact the Project Training Manager, **Nigel Jones** at or Tel: +44 7786 317995 for further information on how to apply for a place on the course.

- VENDOR TRAINING

7-10 September 2009

EnCase® v6 Computer Forensics I

Centro de Convenciones Mapfre, Avda. General Perón, 40 – 28020 Madrid, Spain

CPE credits: 32

Level: Introductory

Prerequisites: Basic computer skills. Advance preparation for this course is not required.

Purpose: This hands-on course involves practical exercises and real-life simulations. The class provides participants with an understanding of the proper handling of digital evidence from the initial seizure of the computer/media to acquisition, and then progresses to the analysis of the data. It concludes with archiving and validating the data. Delivery method: Group-Live. NASBA defined level: basic.

Web site: <http://www.cybex.es>

Section Editor: Mr. Stephen Mason

The reader is invited to send details of conferences, university degree courses, legal training seminars and vendor seminars direct to the editor for inclusion in future issues of the eNewsletter. By submitting your event or course, you accept that it will not necessarily be included in a future issue of the eNewsletter. The inclusion of events and courses is at the sole discretion of the Editor. The criteria for inclusion of events and courses focuses on what, if any, relevance it will have for judges, lawyers and digital evidence specialists within the legal framework.



Editors

A team of seven Editors has been engaged to create the European Electronic Newsletter on the Fight Against Cybercrime, each one being an Expert on the ENAC Section of which they are responsible.

The Editors are in charge of recruiting writers and articles and reviewing and selecting the most appropriate to be included in the ENAC.

According to the order of appearance of their Sections in the ENAC, the Editors are the following:



Mr. PEDRO VERDELHO
Public Prosecutor and trainer
Editors Board Member
Section in ENAC: Legal
pedro.verdelho@gmail.com



Mrs. ELENA DOMÍNGUEZ PECO
Public Prosecutor and Collaborator
for the Spanish Data Protection Agency
elena.dominguez@comjib.org



Mr. MATIAS BEVILACQUA
Computer Forensic Expert
IT Manager
Cybex
mbevilacqua@cybex.es



Mr. NIGEL JONES
Director
Technology Risk Limited
nigel.jones@technologyrisklimited.co.uk



Mrs. LILJANA SELINSEK
Assistant Professor at the
Law Faculty of University of Maribor
liljana.selinsek@uni-mb.si



STEPHEN MASON
Barrister
Chambers of Stephen Mason
stephenmason@stephenmason.eu



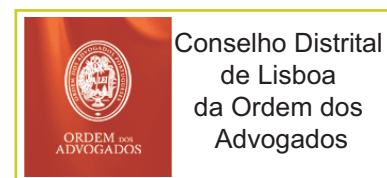
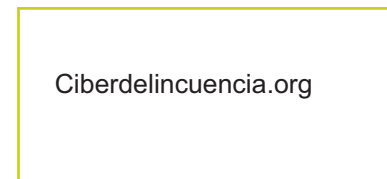
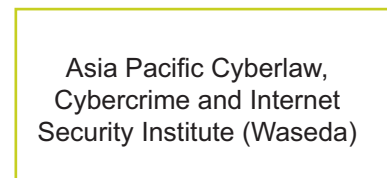
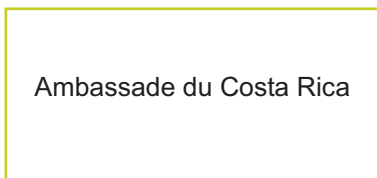
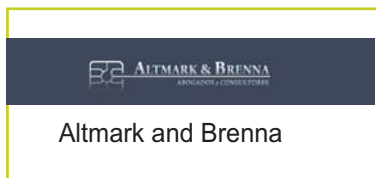
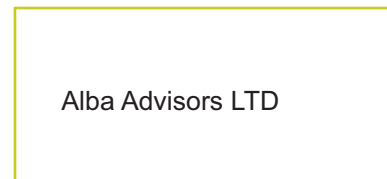
Mrs. MIREIA CASANOVAS
ENAC Chief Editor
Cybex
mcasanovas@cybex.es

Distributors

To ensure the widest possible diffusion of the Electronic Newsletter on the Fight Against Cybercrime, the ENAC counts with the collaboration of Distributor Institutions and Organizations, who will distribute the ENAC monthly to their contacts database.

If you are interested in being a Distributor partner please contact the Project Coordinator Mrs. Mireia Casanovas at mcasanovas@cybex.es.

The Distributors of the ENAC Project are the following:





Council of Europe



Crown Prosecution Service
United Kingdom

Cuerpo Nacional de Policía Española

Cyprus Police
Cyber Crime Task Force



Department for International and European Affairs
Hungary

Directorate for Investigation of Organized Crime and Terrorism
Prosecutor's Office · High Court of Cassation and Justice

Ebay



Escuela Judicial del Consejo General del Poder Judicial



Espion LTD



Estonian Public Service Academy (EPSA)



EUROJUST

Federal Judicial Police
Computer Crime Unit
DJF/FCCU
Belgium



Federal Judicial Police Brazil

Fiscalía General del Estado Ecuador

Fiscalía General del Estado España



Guardia Civil Española
Grupo de Delitos Telemáticos

Home Office
United Kingdom

Institute for Arbitration and Mediation

Institute of Criminal Sciences
Croatia



Institute of Criminology
Faculty of Law · Ljubljana



Instituto Nacional de Tecnologías de la Comunicación INTECO



International Training
and Methodology
Centre for Financial
Monitoring




Ledjit
Consulting

Lithuanian Bar Association



Malta
Police Force



Microsoft

Ministero della Giustizia
Dipartimento per gli Affari
di Giustizia

Ministry of Justice
and Citizens Liberties
Romania

Ministerio Público de Chile
Unidad Especializada en
Lavado de Dinero,
Delitos Económicos y
Crimen Organizado

Ministry of Justice
of the Slovak Republic

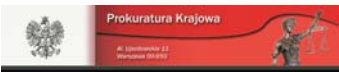


MORENETS CONSULTING
Morenets Consulting

National Institute of Criminology
Budapest



National
Prosecuting
Authority of
South Africa



Prokuratura Krajowa
National Public Prosecutor's
Office of the Republic of Poland

National School for the Judiciary
France



NACPEC.ORG®
North American Consumer
Project on Electronic Commerce



Organization for Security
and Cooperation in Europe



PAD-ORION
Consultores
PAD-ORION

Policía Federal Preventive
Delegación Coyoacán



MINISTERIO
PÚBLICO
Procuraduría General de la
República Dominicana



RISK ANALYSIS CONSULTANTS
Risk Analysis Consultants
s.r.o. · RAC



SERIOUS ORGANIZED CRIME AGENCY
Serious Organized Crime
Agency (SOCA)



Sindicatos dos Magistrados
do Ministerio Publico
Portugal

State Prosecutor
Department of Justice
Philippines

SUSCERTE
Superintendencia de
Servicios de
Certificación Electrónica



Technology
Risk Limited

Telecommunication
Authority
Turkey



TEUTAS srl



The Voivodeship
Headquarters
of the Police
Krakow



unieri
advancing security, serving justice,
building peace

United Nations Interregional
Crime and Justice Research
Institute · UNICRI



University of Buenos Aires



University of Edinburgh



UNIVERSITA V MARIBOR
PRAVNA FAKULTETA
UNIVERSITY OF MARIBOR
FACULTY OF LAW

University of Maribor



University
of Verona



UNODC

United Nations Office on Drugs and Crime

United Nations Office
on Drugs and Crime



Disclaimer:

ENAC e-newsletter provides news and opinion articles as a service to the readers. Statements and opinions expressed in these articles are solely those of the author or authors and may not be shared by the ENAC Board of Editors, Cybex management or the European Commission.

The translations included in the ENAC newsletter were prepared with the utmost care. However, ENAC Board of Editors, Cybex management or the European Commission do not accept any liability for the accuracy and completeness of the compilation and content of these translations, or the direct or indirect consequences of acting or failing to act based on these translations.

Design: © Cybex 2009. All rights reserved

Articles: © 2009. Protected by Law

DL: B.25824-2009
ISSN: 2013-5327



Criminal Justice 2008

With financial support from Criminal Justice Programme
European Commission - Directorate - General Justice, Freedom and Security



cybex

The Digital Forensic Company