ARTICLE:

Online searches and online surveillance: the use of trojans and other types of malware as means of obtaining evidence in criminal proceedings

By **Giuseppe Vaciago and David Silva Ramalho**

Introduction

The development of criminal procedure is determined by the options made by the legislator in the constant conflict between two of the State's constitutional obligations: on the one hand, the obligation to promote internal security and increase the effectiveness in the prosecution of crimes as a means of defending the State's institutions; on the other hand, the obligation to safeguard the citizens' fundamental rights against disproportionate restrictions as a means of protecting justice and freedom. The reconciliation of these conflicting interests is not a matter of seeking balance between them, as much as it is an option of policy to give priority to one over the other in certain circumstances and within specific constitutional limits. The factors that guide the policy include, but are not limited to, the seriousness of the crimes under investigation, the means used to perpetrate them, and the difficulty in collecting evidence.

In recent years, the rapid evolution and dissemination of technology and its misuse by organized crime in order to frustrate criminal investigations has led to a growing prevalence of the first of the abovementioned obligations over the latter, thus justifying the repeated emergence of new and more invasive tools for obtaining evidence. These tools usually emerge in one of three ways: (i) either they are used by law enforcement without a legal basis, (ii) or they are legally framed in provisions meant for different tools for obtaining evidence, (iii) or they are subject to specific legislation.

This has been the case for the use of malware by law enforcement. It has been established that this is a tool of unparalleled effectiveness in facing the – sometimes insurmountable – effects of anti-forensic measures apt to hide, alter, destroy or render impossible to obtain evidence of serious crimes. It has also been established that the use of this technology by law enforcement is spreading across different countries, including in Europe. The debate should now focus on the terms in which it may be constitutionally viable and on the need to correctly legislate on this matter, in order to prevent its illegal and disproportionate use.

Malware

Malware is short for malicious software and it may be briefly described as a 'a simple or self-replicating program, which discreetly installs itself in a data processing system, without the users' knowledge or consent, with a view to either endangering data confidentiality, data integrity and system availability or making sure that the users are framed for a computer crime'.[1] In broad terms, it includes all kinds of software installed surreptitiously by third parties on a computer system, which can be used to somehow compromise its functions, circumvent its access controls, be detrimental to its user or to the infected computer system, monitor the user's activity or appropriate, corrupt, delete and change computer data.

When referring to the use of such software in criminal investigations, the doctrine usually refers only to Trojan horses or simply trojans. However, trojans represent just one of many types of malware which may be used in criminal investigations in the digital environment, alongside, among others, logic bombs, spyware, rootkits, viruses, worms or even the increasingly common blended threats, which include more than one type of malware.

Starting with the most used concept, Trojan horses, we can seek to define them as a type of malware that appears to be harmless and deceives the user in order to stimulate an active conduct that will result in its installation on the target computer system.[2] This

[1] Eric Filiol, *Computer Viruses: from theory to application* (Springer, 2005), p. 86.

[2] This is often provoked by different ways of social engineering, designed to exploit 'vulnerabilities in human beings, which are also a

installation may be made, for example, by simply downloading an attachment to an e-mail message[3] or opening a web page infected with malicious code (for example, in the case of drive-by downloads). Often Trojans are used to create backdoors in the infected computer system, that is, hidden ways to remotely access the system, bypassing the existing authentication mechanisms.[4] Through access afforded by the Trojan horse, the third-party may collect information such as credentials to access restricted websites (including webmails, blogs or social network profiles), he may install different types of malware (such as spyware, keyloggers,[5] viruses or worms[6]), or he may monitor the user's activity on the computer system infected, or even serve as a method for the attacker to browse the Internet anonymously, sending information from the infected computer.

Installation and functioning

As previously mentioned, there are several ways through which malware may be installed in a computer system. In this segment we will cover the three main models of infection, namely the infection via removable hardware, infection via web browser and infection via voluntary download.

Before the advent of the Internet, the model of infection via removable hardware, usually associated with self-replicating malware (such as viruses and worms), was the most common. This would occur through the use of floppy disks, CDs or other media intended to be physically connected to computer systems. This mode of propagation, although comparatively less significant, lingers today and may even be a powerful method to infect local area networks (so-called Local Area Networks or LAN) or disconnected systems of the Internet, as in the case of Stuxnet and Flame.[7] This model proves particularly useful for criminal investigation purposes, since it allows for law enforcement to more accurately reach the intended computer system, thus avoiding accidental infection of other computers.[8]

The second installation model is the drive-by download, in which a user mistakenly believes to be opening a harmless webpage,[9] when in fact he is viewing a webpage partially infected with malicious code which explores vulnerabilities or poorly configured settings[10] in order to infect the target computer system with malware.[11] Another aspect of this model includes automatic downloading of malware when the user attempts to click on a link, usually advertising (called 'malvertising').

The potential of this model for criminal purposes was highlighted by the FBI in August 2013, through the implementation of a form of malware called Magneto in the Freedom Hosting servers, a provider of storage services that contained several hidden services dedicated to child pornography. The malware that was installed exploited a vulnerability in the Firefox browser version 17 and allowed the FBI to identify the MAC address[12] and the Windows administrator user name of the computer system used to access these hidden services, in order to subsequently discover the true IP address.

Finally, malware may also be installed in a computer system by downloading certain files, namely by

part of the system in a broader sense' – Miguel Pupo Correia and Paulo Jorge Sousa, *Segurança no Software* (FCA, 2010), p. 16.

[3] 'Trojan horses do not need to use technical artifices to disseminate themselves, as it is the users themselves who install them freely. Thus, the replication capacity of a Trojan horse depends, above all, on its ability to entice users. This enticement is done through its alleged useful effects, which often lead users, as a gesture of goodwill, to share the application with its colleagues, friends and contacts*'* – Osvaldo Santos, *Firewalls – Soluções Práticas* (FCA, 2011), p. 39.

[4] For example, the Trojan Back Orifice 2000, which was usually spread as an attachment to email messages, allowed the hacker to collect information on the infected computer, as well as to execute commands on the system, redirect internet traffic and reconfigure the infected computer system's settings – Eric Sinrod and William P. Reilly, 'Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws', *Santa Clara Computer and High Technology Law Journal*, Vol. 16, no. 2, 2000, pp. 177-232.

[5] The term keylogger is short for keystroke logging. It is a type of malware that records and sends information on the keys pressed by the user of a computer system, in order to monitor and document the activity undertaken by the user, as well as obtaining passwords and other relevant information that has been entered via the keyboard.

[6] Susan Landau, *Surveillance or Security – The risks Posed by new Wiretapping Technologies* (MIT Press, 2010), p. 54.

[7] Though Flame also worked via Bluetooth – Will Gradigo and others, *Blackhatonomics – An Inside Look at the Economics of Cybercrime* (Elsevier, 2013), p. 37.

[8] Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response* (2012), p. 264.

[9] It may even be the case that a user is effectively trying to access a harmless webpage, for which redirection techniques have been used in order to forward the user to a webpage with malware – Michael Davis, Sean Bodmer and Aaron Lemasters, *Hacking Exposed – Malware & Rootkits Security & Secret Solutions*, McGraw-Hill, 2010, pp. 54-55.

[10] Eoghan Casey, *Digital Evidence and Computer Crime – Forensic Science, Computers and the Internet* (3rd ed., Elsevier, 2011), p. 377.

[11] Eoghan Casey, *Digital Evidence and Computer Crime – Forensic Science, Computers and the Internet*, p. 377.

[12] 'The Media Access Control (MAC) addresses described earlier in this chapter are part of the data-link layer and can be used to identify a specific computer on a network. These addresses are more identifying than network layer addresses (e.g., IP addresses) because they are generally associated with hardware inside the computer (IP addresses can be reassigned to different computers).' - Eoghan Casey, *Digital Evidence and Computer Crime – Forensic Science, Computers and the Internet*, p. 624.

opening some attachments in e-mail messages, either through downloading executable programs (usually pirated or free and obtained through peer-to-peer programs) or even through false legitimate software updates (this was the option chosen by the German police to install the malware known as Bundestrojaner[13]).

Once installed on the target computer system, malware may undertake a number of measures in order to remain undetectable, such as functioning under a seemingly harmless name, looking for ongoing tasks in the system so as to disable tasks commonly associated with antivirus programs, or substituting themselves for a trusted software, so that, after consulting the running software, the user does not suspect that malware is being executed (a technique called process replacement).

Malware execution, generally in the case of Trojans, may include a communication to an external controlling entity with a view to obtaining further instructions or sending additional malware. Depending on the commands sent or malware to be installed, the remote controller may register the user keystrokes (using keyloggers), monitor their activity in real time, listen to the target's conversations via Skype or other Voice-over-IP (VoIP) software or even activate the webcam or microphone on the infected computer system.[14]

Case study: Hacking Team in Italy

At 1h26 in the morning of Monday, 6 July 2015, the following tweet was sent from the account of Hacking Team, one of the most important private intelligence companies: 'Since we have nothing to hide, we will publish all our e-mails, files and source codes'. From that moment onward, in the eyes of experts, Hacking Team turned into 'Hacked Team'.[15] More than one million e-mails were made available on WikiLeaks, for a total 400 Gigabytes of deleted and published company documentation.[16]

The main activity of Hacking Team is marketing the 'Remote Control System Galileo' software (likewise termed 'RCS Galileo'), a high-profile attack tool capable of infecting any type of device (from computers to tablets and smartphones). The operation takes place via the installation of a Trojan on the target device. The malware, in itself, is no novelty, but the intuition of Hacking Team is revolutionary: flanking highly sophisticated attack tools with a simplified dashboard capable of being used even by those other than IT experts. Within a period of two weeks, the intelligence agent is ready to use the program.

It is a technique born in the underground world of hackers, but now used by States as well. The difference is that hackers do it for their own benefit, for profit or for some ideal. Hacking Team, instead, is authorized by governments. If hackers are pirates, Hacking Team is a corsair. Just like the corsair, it may sometimes come under attack by pirates.[17]

The attack mounted against Hacking Team has brought to light a scenario in which governments, judicial authorities, private companies and private citizens throughout the world, without abiding by any protocols, may intercept our conversations, film us through our smartphone cameras, follow our whereabouts using GPS, and listen to us by turning the cell phone into a recorder.

At the international level, what undoubtedly stands out are the relationships entertained by Hacking Team with the Sudanese Government and the Russian Government, without however underestimating its relationships with the governments of Honduras, Ecuador, Panama as well as the Kurdish government. However, Hacking Team does not limited itself to selling software to third countries not found on the 'white-list', but it has also acted in concert with a very large number of Italian judicial authorities in providing information relevant to gathering proof about some of the most important judicial cases in the country.

Among them, we should certainly make mention of the 'Bisignani' case, where an investigation was conducted into a criminal organization, by virtue of which the accused allegedly set up, thanks to an intricate network of influential friendships, a parallel IT system to obtain favours or other services from representatives of politics and industry. In the

[13] Giuseppe Vaciago, *Digital Forensics, Italian Criminal Procedure and Due Process Rights in the Cyber Age*, G. Giappichelli Editore, 2012, p. 125 and David Silva Ramalho, 'The use of malware as a means of obtaining evidence in Portuguese criminal proceedings', *Digital Evidence and Electronic Signatures Law Review*, 11 (2014), pp. 60-63.

[14] Marco Gercke, Understanding Cybercrime Phenomena, Challenges and Legal Response (2012), p. 64.

[15] C. Frediani, ed, *Attacco ai pirati. L'affondamento di Hacking Team: tutti i segreti del datagate italiano* (Lastampa/40k, 2015), p. 8.

[16] It is possible to peruse the deleted e-mails at https://wikileaks.org/hackingteam/emails/.

[17] C. Frediani, ed, *Attacco ai pirati. L'affondamento di Hacking Team: tutti i segreti del datagate italiano*, (Lastampa/40k, 2015), p. 14.

'Bisignani' case, the judge in charge of preliminary investigations did not define such activities as surveillance in a technical sense, essentially leaving to the Public Prosecutor the power to promote such investigative activity in a fully autonomous manner, unlike what is happening in electronic or IT surveillance through less invasive tools of RCS Galileo software.[18]

It is likewise worth mentioning the murder of Yara Gambirasio, a young Italian woman who disappeared on 26 November 2010 in a town near Bergamo, and was discovered dead only a few months later. The case gained substantial media exposure, besides the victim's tender age, on account of the brutality of the crime. The related judicial proceedings ended in July 2016,[19] following a long investigative and judicial process, with a sentence of life imprisonment against the accused Giuseppe Bossetti. During the trial, it emerged that some digital evidence had been gathered through the use of RCS Galileo software installed on the accused's personal computer. The lawyers tried, unsuccessfully, to argue the doctrine of 'evidence planting', alleging that the very moment possession of the device was seized through the RCS Galileo software, it would in theory be possible to insert or create evidence capable of proving the crime charged. Although this defensive motion was disregarded by the court in that specific matter, we cannot exclude the hypothesis that in the near future challenges will be upheld on the basis of the doctrine (quite widespread in common law systems) that evidence gathered with the assistance of illegally obtained information is capable of being excluded from trial. This doctrine is in conflict with the principle, extensively applied by Italian case law, of 'Mala Captum, bene Retentum' by virtue of which an item of evidence, even though acquired in breach of the law, may be used by the court in its decision.[20]

It is difficult to predict what the future of Italian and European rulings might be, but what is certain is that in the years to come this new investigative tool will be carefully analysed by courts all over the world and, wherever possible, limited in its scope of application of ensuring compliance with fundamental individual rights, especially as regards the fundamental rights of a suspect.

Lastly, an analysis should also be conducted on another side effect arising from the attack against Hacking Team. Since the source code of RCS Galileo was made available to the public, many cyber-criminals have used it to penetrate devices with impunity. A recent study of Trend Micro has shown that, only a few days after the leak, many software houses and providers were forced to put out patches to keep their users from getting infected.[21]

Use of malware in Europe

Italian case decisions

In Italy, owing to the Hacking Team leak described in the preceding section, it was at last possible to realize the full extent to which this kind of tool was being used by the judicial authority and the governmental agencies. Despite such a massive use, documented by the publicized e-mails, decisions handed down in cases have nevertheless tackled the issue only sporadically. In the first decision in 2009,[22] the Italian Supreme Court did not find any kind of surveillance in the tools, based on the assumption that the investigative activity consisted of seizing and copying documents stored on the hard disk of the device used by the accused, and did not involve any 'flow of communications', but only 'an operational relationship between the microprocessor and video of the electronic system'. This definition enabled the Public Prosecutor to avoid seeking a search warrant from the judge in charge of Preliminary Investigations to activate such a kind of tool. The case arose from the use, by the Judiciary Police, of a tool capable of acquiring the files stored inside the personal computer used by one of the suspects and located at his workplace. This is an unusual decision in that it does not consider the possibility of not only acquiring the files actually present inside a digital device, but also future files.

[18] A. Testaguzza, *I Sistemi di Controllo Remoto: fra normativa e prassi*, in *Diritto penale e processo* (2014, n. 6, IPSOA), p. 759.

[19] The reasons supporting the decision are yet to be made public at the time of publishing this paper.

[20] To analyse the conflict between the two principles, the reader is advised to read the judgment by the European Court of Human Rights, 30 June 2008, *Gäfgen v Germany*, (Application no. 22978/05), rectified 30 June 2010 under Rule 81 of the Rules of Court.

[21] J. C. Chen, *Hacking Team Flash Attacks Spread: Compromised TV and Government-RelatedSites in Hong Kong and Taiwan Lead to PoisonIvy*, July, 28 2016, available at http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-flash-attacks-spread-compromised-tv-and-government-sites-in-hong-kong-and-taiwan-lead-to-poisonivy/#.

[22] Italian Supreme Court of Cassation, Division V, Decision No. 24695, of 14 October 2009.

Three years later, a new decision by the Supreme Court[23] endorsed this approach in a more famous case in Italy, inasmuch as the investigation involved the 'Bisignani' case cited in the first section above and relating to a judicial investigation about an alleged criminal organisation said to have operated within the sphere of the Italian public administration and the justice system for corruption purposes. In this case, too, it was not deemed necessary to seek a search warrant from the judge, but an order by the Public Prosecutor having been deemed enough.

It took three more years before these two Supreme Court precedents were called into question. In 2015, the Italian Supreme Court of Cassation[24] held that the evidence acquired by using the tools fall within 'electronic surveillance' and that such instances of surveillance should take place in clearly circumscribed places, identified at the outset, and not wherever the subject might be. This decision concerned a delicate case of an organised criminal organisation, and has aroused several debates at national level.

Less than a year later, in a similar case, the decision was made to remit the issue to the 'Joint Sessions' (SS.UU.), i.e., the most authoritative session of the Italian Supreme Court of Cassation, that is involved whenever the need arises to settle conflicts generated by decisions of the individual sessions, or whenever the issues raised have special importance.

The question posed to the 'Joint Sessions' was the following: is it possible to carry out electronic surveillance among people present through the installation of this kind of tool on portable electronic devices (smartphones, tablets or laptops) even in private dwellings, albeit not identified separately and even if no criminal activity is undertaken inside them?

The answer was clear-cut, since the Joint Sessions have expressly countenanced[25] that possibility wherever the crime is particularly serious and falls within the concept of organized crimes, including terrorist crimes, under article 51(3-bis) and (3-quarter) of the Italian Code of Criminal Procedure; essentially, nearly every type of criminal organisation and not only a Mafia-style one. The reasons behind this decision concern the fact that, according to the interpretation of the court, surveillance through malware disregards any reference to the place, being an intrinsically 'roving' electronic surveillance.

This decision has the merit of educating law enforcement agents on the issue, having clarified that such tools may be divided into two categories based on the operational modes of the instrument: 'online search' and 'online surveillance'.

Tools falling in the category of online search (data acquisition modality) make it possible to make a copy, total or partial, of the memory units of the computer system identified as the target; the data and information are then transmitted, in real time or at scheduled intervals, to the investigation bodies through the Internet network in a hidden and protected mode.

Through the tools that carry out online surveillance (information flows interception mode), it is instead possible to intercept the information flow taking place between devices (video, keyboard, microphone, webcam, etc.) and the microprocessor of the target device, thereby allowing the remote control centre to monitor in real time whatever is displayed on the screen (screenshot), keyed in through the keyboard (keylogger), verbalized through the microphone, or seen through the webcam of the target system under surveillance.

In addition to case decisions, during the last year in Italy there has been a succession of four draft laws to bring the investigative tool within the scope of the Italian Code of Criminal Procedure: the first draft law was presented as part of a new law on responding to terrorism.[26] In this draft law, a misguided attempt was made to add into article 266-bis that regulates computer surveillance, the capability of carrying out such type of activity 'also through the use of a tool or software for the remote acquisition of the communications and data found in a computer system'. Fortunately, this amendment was criticised by several members of Parliament and by the Prime Minister himself, inasmuch as it introduced the possibility of undertaking utterly invasive activities vis-à-vis citizens without any legal guarantee other than that of viewing such a tool as a mere instance of electronic surveillance. The same fate was met by the 'Greco' Bill of 2 December 2015.[27]

[23] Italian Supreme Court of Cassation, Division VI, Bisignani Case - Decision No. 254865, of 27 November 2012.

[24] Italian Supreme Court of Cassation, Division VI, Musumeci Case - Decision No. 27100, of 26 May 2015.

[25] Italian Supreme Court of Cassation, Joint Sessions, Scurato Case - Decision No. 1 July 2016.

[26] Decree-Law No. 7 of 18 February 2015, 'Misure urgenti per il contrasto al terrorismo anche di matrice internazionale'.

[27] 'Greco' Bill, of 2 December 2015, Modifica all'articolo 266-bis del codice di procedura penale, in materia di intercettazione e di comunicazioni informatiche o telematiche, available at

At the beginning of 2016, two draft laws were developed ('Casson' amendment[28] and 'Quintarelli' draft law[29]) with a seemingly different approach from the ones of the previous year. Though still being debated, and not in their final versions, what emerges is the need to regulate this tool in an effective way.

As we can see, from the 2009 decision and the 2015 draft laws, a process has been embarked upon that aims to bring the use of the tool into compliance with the fundamental rights of the suspect guaranteed by the Italian Constitution and the European Convention for the Protection of Human Rights. We trust that these laudable aims will then be put into practice.

The 2015 reform on the Spanish Code of Criminal Procedure

For several years the Spanish Code of Criminal Procedure was highly criticized due to its inability to keep pace with the evolution of technology.[30] The Spanish legislator's general lack of activity confronted law enforcement and jurisprudence with a choice between conformity with ineffectiveness or the use of new tools for collecting evidence without specific legal basis. The choice fell on the latter. Thus, gradually the Spanish courts began compensating for the inadequacy of its legislation by allowing the use of new investigative technologies, with a broad legal interpretation of the existing legislation and the Spanish Constitution.[31]

With the increasing use of malware by law enforcement across Europe, the question of whether Spanish courts would find it admissible, even though no legal basis existed for it, began being discussed by Spanish doctrine. While some found this to be inadmissible, others defended the opposite based on the possibility of an analogical interpretation of the legal provisions and case law that allowed for the interception of electronic communications (as long as certain conditions were satisfied, such as precedence of judicial authorization; exclusive use in the case of serious offences; respect for the suspect's defence rights, etc.).[32] In 2011, the Spanish Constitutional Court appeared to admit this possibility when it mentioned that 'it would appear that any interference with the contents of a personal computer – whether via remote access through technical means, and, as in this case, via manually should come legitimated by the consent in principle of the owner, or by the concurrence of the qualifying budgets mentioned above'.[33]

Also in 2011, the Council of Ministers approved a preliminary draft with a new reform on the Code of Criminal Procedure, with the explicit intent to update the legal framework on investigative measures to the challenges posed by new information technologies and by the digital environment in the 21st century. Though this draft was an important step forward in the Spanish legislation, it was still not clear on the possibility of the use of malware as a tool for obtaining evidence.[34] The draft bill did not survive the term of the legislature and was subsequently dropped.

In 2012, the Council of Ministers agreed on the creation of an institutional commission for the preparation of a new Code of Criminal Procedure. The following year, a draft bill was presented to the Ministry of Justice, in which the use of malware was subject to specific and extensive regulation.

The fact that the new Code of Criminal Procedure includes a serious change of the criminal justice system meant that it could not be approved before an acceptable time of public debate and information had occurred.[35] However, the urgency in altering the status quo was not reconcilable with the time needed for consensus on the new Code to be reached. For this reason, while the new Code was being discussed, the Spanish legislator approved a reform of the Spanish Code of Criminal Procedure, by means of the Ley Organica 13/2015.

The new Law includes a chapter dedicated to remote searches on computer systems, which includes specific regulation on the prerequisites for the use of malware, as well as on the duty of collaboration impending on third parties, and on the maximum

http://www.camera.it/_dati/leg17/lavori/stampati/pdf/17PDL0037810.pdf.

[28] The bill and the related MP Casson amendment are available at http://parlamento17.openpolis.it/singolo_atto/53883.

[29] Although the draft law is not yet public, the essential contents are set out inside the text.

[30] Cristina Zoco Zabala, *Nuevas Tecnologias y control de las comunicaciones*, Aranzadi, 2015, pp. 23-25.

[31] Juan Carlos Ortiz Pradillo, *Problemas Procesales de la Ciberdelincuencia* (Editorial Colex, 2013), pp. 170-193.

[32] Eloy Velasco Nuñez, *Delitos Cometidos a traves de Internet: Cuestiones Procesales* (2013), pp. 136-137.

[32] TC, 173/2011.

[33] TC, 173/2011.

[34] Juan Carlos Ortiz Pradillo, *Problemas Procesales de la Ciberdelincuencia*, p. 194.

[35] Cristina Zoco Zabala, *Nuevas Tecnologias y control de las comunicaciones*,p. 25.

duration of the use of this tool (articles 588 septies a. do 588 septies c). With regard to the prerequisites for the use of malware, article 588 septies a. states the following:

> ‘1. El juez competente podrá autorizar la utilización de datos de identificación y códigos, así como la instalación de un software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos, siempre que persiga la investigación de alguno de los siguientes delitos:
>
> > a) Delitos cometidos en el seno de organizaciones criminales.
> >
> > b) Delitos de terrorismo.
> >
> > c) Delitos cometidos contra menores o personas con capacidad modificada judicialmente.
> >
> > d) Delitos contra la Constitución, de traición y relativos a la defensa nacional.
>
> e) Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.
>
> 2. La resolución judicial que autorice el registro deberá especificar:
>
> > a) Los ordenadores, dispositivos electrónicos, sistemas informáticos o parte de los mismos, medios informáticos de almacenamiento de datos o bases de datos, datos u otros contenidos digitales objeto de la medida.
> >
> > b) El alcance de la misma, la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutará el control de la información.
> >
> > c) Los agentes autorizados para la ejecución de la medida.
> >
> > d) La autorización, en su caso, para la realización y conservación de copias de los datos informáticos.
> >
> > e) Las medidas precisas para la preservación de la integridad de los datos almacenados, así como para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso.
>
> 3. Cuando los agentes que lleven a cabo el registro remoto tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo, pondrán este hecho en conocimiento del juez, quien podrá autorizar una ampliación de los términos del registro.’
>
> ‘1. The competent judge may authorize the use of identification codes and data, as well as the installation of a software, enabling, in a remote and telematical manner, examination at a distance and without knowledge of the owner or the user of a computer, electronic device, computer system, mass storage device of computer data or database, always to continue the investigation of any of the following crimes:
>
> > a) Crimes committed within criminal organizations.
> >
> > b) Crimes of terrorism.
> >
> > c) Crimes committed against minors or persons with judicially modified legal capacity.
> >
> > e) Crimes against the Constitution, of treason and related to national defence.
> >
> > f) Crimes committed through the use of computer tools or other information technology or telecommunication or communication service.
>
> 2. The judicial decision authorizing the registration shall specify:
>
> > a) the computers, electronic devices, computer systems or other parts, data storage media or computer databases, data or other digital content subject to the measure;

> b) Its scope, the manner in which data or computer files relevant to the cause are accessed and seized, and the software through which control of information will be executed.
>
> c) Agents who are authorized to implement the measure.
>
> d) The authorization, if any, for the realization and maintenance of copies of computer data.
>
> e) The necessary measures for the preservation of the integrity of stored data, as well as the inaccessibility or deletion of such data from the computer system to which access has been gained.’
>
> 3. Where agents who carry out remote logging have reason to believe that the data sought is stored in another computer system or part thereof, they will present this fact to the judge, who may authorize an extension of the terms of registry.’

The new law also establishes a duty of third-party collaboration, in particular regarding service providers, as well as a one month time limit for the use of this measure, renewable for equal periods up to a maximum of three months (article 588 septies b. and c.).

Other legal experiences

In France, the use of malware was included in the reform to the Criminal Procedure Code conducted by Law No. 2011-267 of 14 March 2011 and it has ever since been regulated in sections 706-102-1 to 706-102- 9 integrated in section 6a, under the heading ‘on the capitation of computer data’.

The use of malware is essentially applicable to organized crime, including, among others, crimes of murder, torture, drug trafficking and theft. The French legal regime requires a prior judicial order in which the reason for the use of this means of collecting evidence must be stated, the reference to the exact location or the detailed description of the targeted computer systems and the duration of the operation, which will have a maximum of four months, renewable for the same period (article 706-102- 1 to 3).

The Estonian Code of Criminal Procedure also provides in its section 1263 (5), that, in the context of surveillance activities, a judge may authorize secret entry into computer systems where such a measure is unavoidable and necessary to achieve the objectives of the surveillance activities. The law also stipulates, in section § 1264 (5) that, whenever installation or removal of technical devices are required for surveillance purposes, the prosecutor must seek independent authorization from the judge expressly for this purpose.

Finally, since 2014, the Finnish Coercive Measures Act also allows for the installation of a device, procedure or program on a computer system for the purpose of technical surveillance (section 26 of Chapter 10 of Law No. 806/2011 called the Coercive Measures Act). The authorization for this purpose covers the hidden entrance into the system in order to bypass, uninstall or otherwise interfere with or undermine the protection of the targeted system.

Conclusions

From this first analysis of the use of malware in criminal investigations, it becomes clear how it is crucial not to underestimate the international relevance and sensitivity of this matter and the importance of legal implementation of technical and procedural requirements for the use of these tools. For this reason, we summarize below some of the main issues that have emerged in countries that envisage these tools in their national legislations:

1. The court order must specify (i) the devices and the data or other digital content subject to the measure; (ii) the scope of the measure, and (iii) the manner in which data relevant to the investigation are accessed and seized.

2. The use of the tool should be limited only to the most serious offences.

3. The measures necessary for the preservation of the integrity of stored data should be set out, as well as the inaccessibility or deletion of such data from the computer system to which access has been gained.

4. A process of certification of the relevant software should be established by recourse to appropriate verification systems ensuring impartiality and confidentiality.

5. Defence lawyers should have the right to obtain the documentation pertaining to all the operations carried out through software and to technically check whether the software in use have been certified.

6. The uninstalling of programs at the end of the authorized use is also required, if need be by providing the user with the information necessary to do so on his own in certain instances.

These topics should be taken into consideration by countries that currently do not have a specific legislation on this matter, so that when the time comes to deal with the complex compromise between the needs of criminal investigation and the protection of fundamental rights, the solution is one that adequately promotes the adequate reconcilement between these conflicting interests.

The authors are members of the editorial board.