Milana PISARIĆ, PhD*
Assistant
University of Novi Sad
Faculty of Law

Review paper
Received: 8 March 2023
Accepted: 12 April 2023
UDK: 343.14:004.056.53
https://doi.org/10.47152/rkkp.61.1.3

THE USE OF HACKING TECHNIQUES FOR THE PURPOSE OF CRIMINAL PROCEDURE

Since certain trends in information technologies significantly hinder criminal investigation, there is an evident need for the creation of an appropriate criminal procedure mechanism to overcome these obstacles. One of the options is to enable the law enforcement agencies to use hacking techniques in order to gain access to protected computer systems, networks and data, even remotely, in order to identify suspects, to monitor their activities and communications, and to collect evidence. In this paper the author is considering the possibilities, advantages and risks of using hacking techniques for the purposes of criminal proceedings. After pointing out the risks of malware use by the competent authorities, the normative framework for overcoming those risks was considered through regulating the authorized access to a protected computer system or network, as a special investigative action, so the data obtained through such actions could be used as evidence in the court of law.

Keywords: criminal procedure, electronic evidence, encryption, lawful hacking.

* E-mail: mpisaric@pf.uns.ac.rs

1. Introduction

Certain trends in the development of information technologies, especially those used to protect the privacy and security of computer systems, networks and data of legitimate users, also benefit the perpetrators of criminal acts, and have led to the fact that the state authorities responsible for detecting and proving criminal acts face with serious obstacles when they need to collect data from such protected systems and networks (Going dark problem, Pisarić, 2020). These tendencies have an extremely negative effect on the practical and technical ability of competent authorities to implement certain investigative measures and actions: a) providers of electronic communication services incorporate, as a default setting, encryption (increasingly end-to-end encryption, E2E) into their products and services - which makes it impossible to carry out covert surveillance of communications (Pisarić, 2022); b) manufacturers and users increasingly apply full disk encryption - which makes it impossible to search the device (Pisarić, 2021:); c) the use of hidden services in the dark web makes it impossible to identify devices and perpetrators;[1] d) the widespread use of mobile devices based on cloud computing makes it difficult to search them and collect computer data in the traditional way;[2] e) the widespread use of wireless networks makes it difficult to conduct covert surveillance of communications conducted at a single network access point, etc. In order to create a balance between technological development and the necessity for competent state authorities to respond adequately, it is quite justified for the legislator to create a legal framework for the collection of electronic evidence despite and in addition to technologies aimed at protecting security and privacy. One of the possible solutions is the mechanism of exceptional access (backdoors), which implies that device manufacturers/service providers are obliged to create an entry point in the device or network for accessing the necessary data without the knowledge and permission of the user (Pell, 2016: 609) Considering that in this way the entire computer system would be weakened, which is the unanimous opinion of the scientific and expert public in the field of information security (Abelson et al., 2015), we should not lose sight of alternative sources of data, which can be used without compromising the protection mecha-

1 In the Tor network, the privacy and security of the IP address, location and usage data of individual users are protected, as well as the privacy and security of the IP addresses of web servers, which host web pages and are called hidden services. In this way, an anonymous, encrypted connection is established - neither the user's IP address is known to the website, nor the server's IP address to the user.

2 Cloud computing service means storing device content on remote servers of the service provider (which are spread around the world) and accessing that content from any device and place with an appropriate connection (e.g. iCloud, Google Drive, OneDrive).

nisms of encryption (Kerr, 2018). Data stored in the cloud,[3] electronic communication metadata,[4] IoT device metadata,[5] etc. most often are not encrypted and represent a significant source of information for the work of law enforcement agencies, without the need to gain access to content protected by encryption. In addition, the legislators of certain countries have regulated the authorization of competent authorities to gain access, that is, to hack into a protected computer system/network (policeware, govware).

2. Malware-based hacking technique

Hacking means gaining access, through manipulation, to a computer data, program, system or network, which is done without the awareness, knowledge, consent and permission of the owner, or user. Access and manipulation are realized by overcoming protection measures in the computer, computer network or electronic data processing, most often by using malicious software, or malware, which is installed on the device in situ, or remotely.[6] Malware is a program code that is based on the exploitation of vulnerabilities, i.e. defects in the software and hardware elements of a computer system/network, which enable an unauthorized person to gain access and undertake activities in a protected computer system or network without the knowledge and consent of the user (often covertly). These vulnerabilities are exploited by using malware locally on the system being attacked (hands-on), or remotely (drive-by) (Bellovin et al., 2014: 23). The most effective use is a zero-day vulnerability, which is detected and exploited before the public or the manufacturer becomes aware of it due to system compromise.[7] There is a whole vulnerability market: the “white” market, where device and application manufacturers or other interested parties are offered vulnerabilities in the amount of several hundred thousand dollars and more, while they, in turn, in order to increase security and protect user privacy, offer monetary rewards for

3 As the content is usually stored in a decrypted form, the competent authorities can request the providers of this service to hand over the necessary data.

4 Metadata is information about electronic communication data, not including the content of the communication. Metadata refers to device location data, IP address of the sender or recipient, etc.

5 The Internet of Things are devices and sensors connected to the Internet or another computer network, such as smart TVs, GPS devices, etc.

6 Malware can be in the form of virus, worm, spyware, ransomware, key logger, etc.

7 Vulnerabilities can be categorized in several ways, and one of the divisions is between vulnerabilities that are known to the manufacturer (n-day vulnerabilities: n-days/old days) and vulnerabilities that are not known to the manufacturer (zero-day vulnerabilities: zero-day/0- days). The process of turning an n-day vulnerability into a zero-day vulnerability is called disclosure.

finding and reporting bugs (bug bounties);[8] the “black” market where vulnerabilities are offered and bought to gain illegal and unauthorized access to the system/network; the “grey” market, where the buying and selling of vulnerabilities takes place between government authorities and individuals and companies that offer products and technologies that are based on the exploitation of vulnerabilities (Anstis, 2021:4).

Unauthorized infiltration into electronic data processing, computer system or network, and access to data stored in the system or transmitted through the network, is undertaken in order to cause damage and/or take control over computer data, system or network. As such, hacking constitutes a criminal act, unless there is appropriate authorization for such an act. Authorization to competent authorities to use hacking techniques (right to hack back) can be given in order to achieve different goals.[9] For the purposes of criminal proceedings, the goal of hacking would be to enable the identification of devices and users in order to discover the perpetrator, or covert surveillance of communications, or search of a device, i.e to enable the obtaining of electronic evidence. In order to understand how this goal can be achieved, it is first necessary to show how hacking using malware takes place. The use of this technique takes place through four stages (Mayer, 2018:583):

1) Malware injection - Competent authorities can install malware in a device via portable hardware (USB, CD) after achieving covert, physical access to the device (in situ), or deliver it remotely to a target szstem/network, in several ways. The phishing technique is aimed at certain users, by “luring” them through a message to download content or visit a website infected with malware, which is then secretly installed in the device (drive-by-download). In the investigation of anonymous online activities, especially hidden services on the dark web, the watering hole technique can be used, which is aimed at all users

8 Companies such as Zerodium and Exodus Intelligence buy zero-day vulnerabilities from hackers and sell them to device manufacturers, law enforcement and security agencies. Monetary fees for a reported vulnerability depend on the operating system, device, application, and type of vulnerability. The highest sums are offered for vulnerabilities in the latest versions of the Android and iOS operating systems - up to two and a half million dollars, and in messaging applications - up to one and a half million dollars for the iMessage and WhatsApp applications.

9 Those goals could be: exercising control over messages (preventing message sending, manipulation of the domain name system, changing the content of the message, “flooding” communication channels, changing the face of the website), causing damage to a certain number of subjects (internal and external modification of physical systems and devices, data modification, service theft), conducting surveillance or collecting data and information (compromising the end device or host, monitoring the communication channel, “breaking” encryption). More on that, Access Now, 2016: 11-12.

who exhibit certain behavior. Namely, after the incriminating website is identified, the competent authorities take control of the server, in order to deliver malware that will exploit vulnerabilities in the browser, after which the malware infects every device whose user visits or logs in to a certain website;

2) Vulnerability exploitation - For the launch and execution of any downloaded/installed software in the computer system, there are certain security restrictions, i.e. the operating system assigns limited permissions to the software so that it can only access certain data and functionalities in the device, thus protecting the user's privacy and security (sandbox). In order for the law enforcement agencies to gain access to the necessary data, it is necessary to overcome these security obstacles, which is why the introduction of malware into the system is followed by the exploitation of vulnerabilities;
3) Task execution - After the security obstacles are bypassed, by exploiting the vulnerability, the malware now equipped with the necessary access permissions, is launched, takes (partial) control over the device and executes the task, i.e. collects data;
4) Reporting - After the launched malware has completed the task, or while the execution is still in progress, the collected data is sent to the server of the law enforcement agencies.

For the purposes of criminal proceedings, malware can be entrusted with a variety of tasks.

If it is necessary to collect data about a user who anonymously uses certain services, the malware collects identifying data about the device and the network (e.g. IP address, MAC address, type and version of the operating system, type and version of the browser, username, URL of the last visited web pages, etc.) and sends them to the server of competent authorities. This data is then used to relate a specific user to a specific device - when a specific IP address is identified, with the help of an Internet access service provider, a specific activity in the online environment is associated with the account, then a specific device associated with that account is identified through the MAC address, and then the user can be identified through the user name that was logged in at a certain time on that device.

Also, the malware can collect data from the device about wireless access points, which are then compared with the external database of service providers, and in this way the physical location of the device can be determined.

Malware can be used to gain access to a device and to collect content stored on a device (thus allowing for covert and remote device search and seizure of

electronic evidence) or data needed to log into a social network account, but also to take control of a camera or microphone (thereby enabling covert surveillance, tracking and recording).

In addition, it is possible for the achieved control to spread from the initially infected device (e.g. computer) to other devices connected to it (e.g. mobile phone) of the same user.

Finally, even when it comes to communication protected by E2E encryption, the use of malware allows the covert surveillance of the communication to be carried out on the end device before being encryped and sent, i.e. after being received and decrypted (Pisarić, 2022).

3. Examples of LEAs using malware-based techniques

Although hacking for the purposes of criminal proceedings has been the subject of a current debate on encryption in the general, professional and scientific public since 2015, as a factor that seriously threatens the criminal investigatoin, there are examples of the use of malware for the purposes of criminal proceedings from an earlier period. Beginning in the late 1990s, authorities in the USA used the Carnivore tool for monitoring traffic in the computer network (the so-called network sniffer) for investigative purposes (Hartzog, 2002). The first known case of the use of malware to overcome the encryption problem dates back to 1999: after searching the suspect's computer, an incriminating file was found, protected by the PGP encryption program, so the police, after receiving approval, secretly installed the KLS (Key Logger System) malware on the computer, which monitored and recorded everything keyboard inputs, including the PGP key code (Carrell, 2002).

Unlike these cases where the malware was physically installed on the suspect's device, in the 2000s malware is starting to be delivered remotely via a computer virus. The FBI first disclosed the use of this technique for remote computer searches in 2003: in Operation Trail Mix, the KLS malware, called Magic Lantern, was used to overcome the problem of protecting the communications of suspects using the PGP program (Curran et al., 2007: 309). In the Timberline case in 2007, the FBI remotely, using the phishing technique, installed the CIPAV[10] malware on the suspect's computer, which collected and sent the necessary data

10 Computer and Internet Protocol Address Verifier.

to their server,[11] on the basis of which the user's data was requested from the Internet access service provider.

It is also known that a malware has been used against an unspecified number of users through the watering hole technique in several cases so far: (a) in Operation Torpedo, 2012 – after the Dutch police gained access to the account of the administrator of a hidden service in Tor (Pedo Board) and located the IP addresses of servers in the USA that hosted a site with child pornography, the FBI was authorized by a court order to install malware (which was based on the exploitation of vulnerabilities in the Adobe Flash Player plug-in for the Tor browser) on hidden services and to apply the network investigative technique (NIT technique) in relation to each computer that accesses that service;[12] (b) in Operation Freedom Hosting, 2013 - the FBI, in cooperation with the French police, applied this technique to users of the Freedom Hosting server that hosted hidden services in the Tor network, including 23 websites with child pornography, by exploiting a vulnerability in the Mozilla Firefox browser in order to collect the IP and MAC addresses of service users;[13] (c) in Operation Pacifier, 2015 – after identifying and taking over the server hosting Playpen, a child pornography site, the FBI, authorized by a court order, continued to host the site for several weeks and, using the NIT technique, collected data on more than 8,000 user computers.[14] In all these cases, after collecting identifying data for individual computers, the police requested information about device users from Internet access service providers.

These examples of hacking by the competent authorities are not isolated precedents, and show that in the last twenty years the possibility of hacking has

11 CIPAV collected IP and MAC address, data about operating system, the browser used, registered computer users and registered computer name, as well as browsing history. More on that, Application and Affidavit for Search Warrant, In the Matter of the Search of Any Computer Accessing Electronic Message(s) Directed to Administrator(s) of MySpace Account “Timberlinebombinfo” and Opening Messages Delivered to That Account by the Government .

12 More on that, Application for a Search Warrant, *In re* Search of Computs. that Access the Website “Hidden Service A” Which Is Located at oqm66m6lyt6vxk7k.onion, No. 8:12MJ360 (D. Neb. Nov.19, 2012); Application for a Search Warrant, *In re* Search of Computs. that Access the Website “Hidden Service B” Which Is Located at s7cgvirtswvojlis.onion, No. 8:12MJ359 (D. Neb. Nov. 19, 2012); Application for a Search Warrant, *In re* Search of Computs. that Access the Website “Bulletin Board A” Located at http://jkpos24pl2r3urlw.onion, No. 8:12MJ3 56 (D. Neb. Nov. 16, 2012).

13 More on that, Application and Affidavit for Search and Seizure Warrant, In the Matter of the Search of the computers that access “Websites 1-23”.

14 More on that, Application and Affidavit for Search Warrant, In the Matter of the Search of Computers that Access upf45jv3bziuctml.onion, No. 1:15-SW-89.

expanded - from the physical installation of “spy” software on a single device (spyware) to the mass infection of devices remotely. In addition, the use of hacking techniques by the law enforcement agencies has contributed to the development of the market for vulnerabilities and hacking products and services. In the future, it is entirely possible for authorities to send commands to a targeted device/ network/account from a central management server, or to require software vendors to include malware in a software update. Although the use of the mentioned and similar techniques should not be denied a priori to competent authorities, the question arises whether it can be justified only by the technological reality of a complex IT environment, i.e. existing and new problems, on the one hand, and techniques for overcoming them, on the other hand. Namely, one must not lose sight of the invasiveness of the hacking techniques described, which implies the potential indiscriminate collection of data. In addition, there is a likelihood that their application will disrupt and/or cause damage to the wider information infrastructure. In other words, the application of hacking techniques by the competent authorities carries with it certain risks.

4. Risks of LEAs using malware-based techniques

At a time when looking for a way to provide LEA the access to protected communications, platforms and devices, prescribing the authorization for the use of hacking techniques, as a way to overcome the problem created by the application of technologies aimed at protecting privacy and security, is a better solution compared to the deliberate creation of new security flaws in the computer system/ network, in the sense of the Backdoor option (Pisarić, 2022:66). Nevertheless, the use of malware that is based on the exploitation even of existing vulnerabilities is not without risks, which can be additionally contributed to by the absence of clear and precise technical and legal rules.

A. Information security risk. The use of malware to gain access to a device/ system/ network carries with it a risk to information security, which goes beyond the specific target and potentially endangers the wider information infrastructure, because it is based on the discovery and exploitation of vulnerabilities. Especially the use of zero-day vulnerabilities creates risks, because they can appear in any software/ hardware, remain undetected for several months, even years, and are not easy to spot. The failure of competent authorities to disclose perceived vulnerabilities to software or hardware manufacturers contributes to the reduction of the general level of information security. Al-

though such an omission of disclosure may be justified by the interests of a specific investigation (but at the same time it allows the LEAs to repeatedly use zero-day vulnerabilities until they are discovered), it essentially makes it impossible for the manufacturer to overcome, i.e. “patches” vulnerabilities, putting all software/hardware users at risk. Also, there are known examples of vulnerabilities that were originally used by the competent authorities getting out of control, that is, they were discovered and used by malicious actors (e.g.: Stuxnet, Petya/Notpetya ransomware, Wannacry ransomware). The mentioned risks could be overcome by creating a system for managing vulnerabilities and prescribing strict legal and technical rules for their exploitation (such as exists, for example, in the USA - Vulnerability Equities Process).

B. Human rights risk. The LEA’s use of hacking techniques is extremely invasive and represent a potential disproportionate interference in individual human rights guaranteed at the international, regional and national level, primarily the right to privacy. With its application, it is possible to collect unlimited data that is stored in the device or transmitted over computer networks, both in relation to the suspect and in relation to legitimate users. As the challenge of detecting the suspect is the principle justification for the introduction of this investigative technique, and as the device used cannot be identified with certainty, there is a real risk that the malware may accidentally compromise the device/data of third parties. This is also contributed by the fact that this technique is to some extent indiscriminate, and that the target can be other users who share the targeted device, system or network. Also, the data obtained from the target device/network may contain sensitive, confidential, even legally privileged or proprietary material. The mentioned risks should be overcome by the norms of criminal procedural law.

C. Extraterritoriality risk. The transnational structure of the Internet, as well as the use of cloud services, require the competent authorities to act extraterritorially in certain cases in order to achieve remote access to computers/networks located abroad (Pisarić, 2016). However, the implementation of authorized hacking in the event that the targeted system/network or user is located outside the jurisdiction of the state where hacking would be permitted, would be contrary to the jurisdictional rules established by international public law (Pisarić, 2019: 228-231). Although it seemed traditional notion of state territory would

become irrelevant in cyberspace and that states could unilaterally prescribe the possibility of extraterritorial action to collect electronic evidence, the use of mechanisms for providing international assistance in criminal matters remains imperative, despite these procedures are slow and impractical. In this sense, it is necessary to improve the rules on mutual assistance in criminal matters in the collection and exchange of electronic evidence.

In order to find a balance between the interests of the criminal procedure and the interests of information security and privacy, it is necessary to create an appropriate legal framework for the use of this investigative technique, taking into account the mentioned risks, and in order to mitigate them, i.e. reduce them to the smallest possible extent. In the following part, the key requirements, to which the regulation of authorized hacking should be addressed, are considered.

5. Authorized access to protected computer system/network

The malware-based hacking techniques could be used to gain access to a protected computer, computer network, or electronic data processing in order to gather evidence. However, it is important to point out the difference between the two cases of hacking by the authorities.

In the first case, malware would be installed remotely into the device in order to gain access to the stored data (in order to remotely search the device and record/remove data) or data transmitted through the network (in order to secretly monitor communication on the end device, i.e. while it is in decrypted form).

In the second case, hacking techniques would be used to achieve access to a device protected by encryption and the data stored in it, which is physically accessible to the competent authority (in order to search the device in situ).

Considering the different degree of intrusiveness, the legal regulation should make a clear demarcation of the use of hacking techniques in these two cases, while taking into account a number of important and complex legal issues: for what purpose the investigative techniques could be applied, which material and formal conditions would have to be met, who would approve the implementation, whether the application would be limited only to certain persons, and how this would be achieved, how the collection of data irrelevant to the specific case would be minimized, etc. Further considerations refer to the first case of the use of hacking techniques, which are based on the use of malware.[15]

15 More about the other case of using hacking techniques and tools for search purposes, see Pisaric, 2021.

In order to create an appropriate legal framework for the use of hacking techniques to gain remote access to a protected computer system/network, it is first necessary to clearly determine the purpose of norming such a use, what would be considered by such an investigative technique, that is, what it would consist of. The meaning of the regulation would be to give a permission to the competent authorities to apply hacking techniques and tools from a distance in order to collect electronic evidence for the purposes of criminal proceedings if it concerns electronic data processing, a computer system or network that are protected by technical protection measures and which prevent or significantly make it difficult to gather evidence by implementing existing investigative measures and actions. In other words, this investigative measure may be considered as an authorized access to a protected computer or computer network for the purpose of searching or secretly monitoring communications.[16] This term is appropriate, because it is technologically neutral and broad enough, so that, in addition to the use of malware, it would also include other tools and techniques, and at the same time sufficiently specific, because it clearly indicates the nature of the activities that the competent authorities would be authorized to undertake.

Since the use of hacking techniques would represent an investigative technique with profound invasiveness, it should not be aimed at intentionally and excessively weakening technical security measures that were primarily established for the protection of user privacy. For this reason, it is necessary to clearly foresee the conditions under which such techniques can be used for the purposes of criminal proceedings. Although it could not be categorically disputed that LEA's hacking would be useful, one must not lose sight of the fact that such an authorization could have a limiting/threatening effect on certain human rights, above all the right to respect for private and family life, freedom of opinion, freedom of expression, freedom of assembly and association, etc. The initial input may be found in international legal standards concerning special investigative measures. Starting from the fact that the ECHR foresees that the limitation of the right to privacy and other relevant rights can be allowed only in certain, exceptional circumstances, the European Court has clearly established in Niemietz v. Germany that the activities of the competent authorities represent a permissible interference with these rights only on the condition that the authority of the competent authorities has a clear legal basis, that they are prescribed for the achievement of a certain

16 Different terms are used to denote this investigative technique: lawful hacking, government hacking, law enforcement hacking, network investigative techniques, remote access search and surveillance, remote computer search, remote search, etc.

legitimate goal and that it is necessary for the achievement of that goal in a democratic society.

Given that the legitimate goal of using the hacking techniques by the competent authorities is the detection and clarification of criminal acts, i.e. the collection of electronic evidence, before such an authorization would be allowed by the law, it is necessary to assess the necessity of such interference with human rights, through an assessment of subsidiarity (that whether there are less intrusive measures and actions for the achievement of the goal), effectiveness (to what extent the action would contribute to the achievement of the goal) and proportionality (to what extent the impact of the action is proportional to the achievement of the goal). In the assessment of subsidiarity, one should not lose sight of the existing investigative techniques and alternative possibilities for collecting the necessary data, which are less invasive to human rights. In addition, it is questionable how effectively this investigative technique would contribute to overcoming technical-technological obstacles to the investigation, primarily encryption.

Although examples of the use of hacking techniques by competent authorities have been known for a long time, the legal regulation in only a few countries is of recent date, so at the moment one can look with caution not only at the effectiveness of those powers, but also at the proportionality of achieving the legitimate goal (Pisarić, 2022:71). However, if despite these reservations, it is accepted that the regulation of the use of hacking techniques is necessary to overcome the problem of “Going into the dark”, the legislator could allow interference with the right to privacy and other relevant rights, by prescribing appropriate restrictions and guarantees. Whereby the legal basis for the use of hacking techniques should not be set too broadly and generally. Namely, starting from the principle of legality, the legal framework should be clear, definite and precise (UN Human Rights Council, 2013; UN General Assembly, 2016), and should contain specific provisions that would regulate hacking as an investigative technique (UN High Commissioner for Human Rights, 2014). In other words, the legislator should regulate the use of malware-hacking hacking techniques for the purposes of criminal proceedings as a special evidentiary action, and the law should establish a mechanism consisting of certain ex-ante and ex-post elements. Examples of conditions that should be met before the use, include: obtaining court approval, limiting the use of hacking techniques to more serious crimes, ensuring that the technique is appropriately targeted against specific persons/devices, limiting the duration of the measure, taking steps to ensure suitability of tools and ensuring deletion of unnecessary or third-party data. Examples of steps that should follow the use, include: notifying the person against whom the measure has been applied,

providing a means for effective monitoring of the implementation of the measure (UN Human Rights Council, 2014).

In case no explicit provisions on lawful lacking exist in the law, the use by analogy of general provisions, which were created for a different, analogous operational environment, could be brought under the “gray zone” , which due to insufficient legislative precision and clarity, would not provide a sufficient and adequate level of human rights protection. On the technical side, special attention should be paid to the acquisition of third-party hacking tools in order not to give legitimacy to the growth and cultivation of the vulnerability market. In this connection, the question of the necessity and method of disclosing vulnerability the competent authorities used is also raised. Careful and comprehensive consideration of these issues can contribute to prescribe in the most correct way the authorization of competent authorities to remotely access protected computer systems/networks/platforms and the data stored in them, or transmitted through them.

6. Conclusion

Considering certain technological tendencies, which were pointed out in the paper, within the debate on the need, measure and way of enabling state bodies to access protected electronic data processing, computer systems and networks, the lawful hacking could be of incomparable usefulness and efficiency for overcoming LEA’s obstacles in digital environment, and at the same time it represents an optimal alternative to encryption restrictions or mandatory exceptional access in terms of Going dark problem. Instead of requiring technology companies to sabotage their own protection mechanisms and thereby compromise users’ security and privacy, this alternative is based on exploiting already existing (often unintentional) vulnerabilities in the system/network. The remote access using hacker techniques may be considered as a legitimate and effective investigative technique that could contribute to overcoming the obstacles that the competent authorities face when discovering the perpetrator, conducting searches of protected computer systems and secret surveillance of electronic communications - if the competent authorities cannot determine the identity or location of the perpetrator with the help of Internet access service providers, they could access his device remotely and find the data needed for identification; if the competent authorities cannot find out the content of the suspect’s communication even through cloud computing service providers, they could gain access to the device and obtain the stored communication and intercept future conversations; if the competent authorities cannot find out the content of the encrypted data that is

stored in the device or transmitted through the network, they could gain access to the device and that data while it is decrypted, or even data needed for decryption.

Although the LEA's use hacking techniques may be a legitimate option, it still lacks the character of legality. Certain risks are immanent in the absence of a clear procedural framework - from the legal side, the potential for endangering human rights, above all the right to privacy and protection of personal data, is far higher compared to the existing investigative techniques; on the technical side, there is a risk of weakening information security. That is why it is necessary to devise an appropriate legal framework for the use of malware for the purpose of gathering evidence, while taking into account the safety and privacy of the user, especially the suspect. When considering what the legal framework governing this investigative technique should look like, it is necessary to take into account several elements. First of all, it is necessary to determine what is meant by this investigative technique, and then, considering the high degree of intrusiveness, enable its use only as an ultima ratio measure (in terms of the principle of subsidiarity), and only for the purpose of discovering and proving more serious crimes (in terms of the principle proportionality). Furthermore, it is necessary to foresee the conditions that must be met in order to be able to grant the authorization, with a clear demarcation between in situ access and remote access. In other words, the regulation governing the criminal procedure should provide for authorized access to a protected computer system/network as a special evidentiary action, and prescribe appropriate ex-ante conditions and ex-post steps.

List of references

- Abelson, H., Anderson, R., Bellovin, S., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Green, M., Landau, S., Neumann, P., Rivest, R., Schiller, J., Schneier, B., Specter, M. & Weitzner D. (2015) *Keys under Doormats: Mandating insecurity by requiring government access to all data and communications*, Cambridge.
- Access Now. (2016) *A human rights response to government hacking*.
- Anstis, S. (2021) Government procurement law and hacking technology: The role of public contracting in regulating an invisible market. *Computer Law & Security Review*, *41*(1), pp. 1-16. https://doi.org/10.1016/j.clsr.2021.105536
- Application and Affidavit for Search and Seizure Warrant, In the Matter of the Search of the computers that access “Websites 1-23”.
- Application and Affidavit for Search Warrant, In the Matter of the Search of Any Computer Accessing Electronic Message(s) Directed to Administrator(s)

of MySpace Account “Timberlinebombinfo” and Opening Messages Delivered to That Account by the Government.
- Application and Affidavit for Search Warrant, In the Matter of the Search of Computers that Access upf45jv3bziuctml.onion, No. 1:15-SW-89.
- Application for a Search Warrant, *In re* Search of Comput. that Access the Website «Bulletin Board A» Located at http://jkpos24pl2r3urlw.onion, No. 8:12MJ3 56 (D. Neb. Nov. 16, 2012).
- Application for a Search Warrant, *In re* Search of Comput. that Access the Website «Hidden Service A» Which Is Located at oqm66m6lyt6vxk7k.onion, No. 8:12MJ360 (D. Neb. Nov. 19, 2012).
- Bellovin, S., Blaze, M., Clark, S. & Landau, S. (2014) Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet. *Northwestern Journal of Technology and Intellectual Property*, *12*(1), pp. 1-64.
- Carrell, N. (2002) Spying on the Mob: United States v. Scarfo - A Constitutional Analysis. *Journal of Law, Technology & Policy*, 1, pp. 193-214.
- Curran, K., Breslin, P., McLaughlin, K. &Tracey G. (2007) Hacking and Eavesdropping. In: *Cyber Warfare and Cyber Terrorism.* New York, pp. 307-317.
- Hartzog, N. (2002) The “Magic Lantern” Revealed: A Report of the FBI’s New “Key Logging” Trojan and Analysis of Its Possible Treatment in a Dynamic Legal Landscape. *Journal of Information Technology & Privacy Law*, *20* (2), pp. 287-320.
- Kerr, O., Schneier, B. (2018) Encryption Workarounds. *Georgetown Law Journal*, 106(4), pp. 989–1019.
- Mayer, J. (2018) Government Hacking. *The Yale Law Journal, 127*(3), pp. 570-662.
- Pell, S. (2016) You Can’t Always Get What You Want: How Will Law Enforcement Get What It Needs in a Post-CALEA, Cybersecurity-Centric Encryption Era?.*North Carolina Journal of Law & Technology*, *17*(4), pp. 599 -609.
- Pisarić, M. (2016) Cross-Border Access to Data as a Way to Collect Electronic Evidence. In: Kolarić, D. (ed). *International scientific conference “Archibald Reiss Days” thematic conference proceedings of international significance* (*3*, pp. 513-520). Belgrade: Academy of Criminalistic and Police Studies.
- Pisarić, M. (2022) Communications Encryption as an Investigative Obstacle. Journal of Criminology and Criminal Law, *60* (1), pp. 61-75. https://doi.org/10.47152/rkkp.60.1.4
- Pisarić, M. (2019) *Eletronski dokazi u krivičnom postupku*. Novi Sad: Pravni fakultet u Novom Sadu.

- Pisarić, M. (2020) Enkripcija kao prepreka otkrivanju i dokazivanju krivičnih dela. *Zbornik radova pravnog fakulteta u Novom Sadu*, *54*(3), pp. 1079-1100. 10.5937/zrpfns54-26929
- Pisarić, M. (2021) Enkripcija mobilnog telefona kao prepreka otkrivanju i dokazivanju krivičnih dela – osvrt na uporedna rešenja. *Anali Pravnog fakulteta u Beogradu*, *69*(2), pp. 391-416. 10.51204/Anali_PFBU_21205A
- Response & Request to Strike Defendant's Request for Daubert Motion, U.S. v. Cottom, No. 8:13-cr-00108-JFB-TDT, at 5 (D. Neb. June 29, 2015).
- UN General Assembly (2016). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. A/71/373.
- UN High Commissioner for Human Rights (2014). *The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights*. A/HRC/27/37.
- UN Human Rights Council (2013). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. A/HRC/23/4.