South American Publishing

SAP Netnography. 2023;1:22
doi: 10.62486/net202322

ORIGINAL

Cybercrime: Ransomware, and government actions for analyzing criminal behavior in the province of Córdoba

Cibercrimen: Ransomware, y las acciones gubernamentales para su análisis de la conducta criminal en la provincia de Córdoba

Agustín Ramiro Manrique Aguad[1]
María Belén Gauna[1]

[1] Universidad Siglo 21, Licenciatura en Criminología y Seguridad. Argentina.

Submitted: 14-03-2023 | Revised: 03-07-2023 | Accepted: 26-10-2023 | Published: 27-10-2023

ABSTRACT

In this paper, government actions aimed at addressing the analysis of criminal behavior by cybercriminals in ransomware attacks through the use of ICT (information and communication technology) in private and public organizations in the province of Córdoba were described. The method used had a qualitative approach of a non- experimental type, with a descriptive and explanatory scope. In addition, as instruments, documents and a semi-structured interview were used. For its part, it was inquired about the application of the operational analysis of cases to this criminal typology by the Judiciary of Córdoba. In addition, the most resonant cases that occurred in Córdoba in the last ten years were established, and the difference between cybercrime and cybercrime of ransomware behavior was delimited. Among the results, there is a coincidence of factors and behaviors between cases and a great contextual influence of the situation in terms of computer security in organizations, in their ability to react. In turn, no information was found that shows that the operational analysis of cases has been used for these crimes in the province of Córdoba. Therefore, doors were opened to new lines of investigation and the creation of new methodologies of governmental approach. Emerging as the main recommendation, the creation of a specific case analysis method for the study of the behavior of cybercriminals and their victims, in order to identify the causal roots of the phenomenon and thus develop more effective government policies for its prevention and control.

Keywords: Cybercrime; Ransomware; Encryption; Cyberattack; Hacker; Malware; Software; ICT; Cyberspace; Cybercriminal.

RESUMEN

En este trabajo, se describieron las acciones gubernamentales tendientes a abordar el análisis de la conducta criminal por parte los ciberdelincuentes en los ataques ransomware mediante el uso de TIC (tecnología de información y comunicación) en organizaciones privadas y públicas, en la provincia de Córdoba. El método utilizado tuvo un enfoque cualitativo de tipo no experimental, con un alcance descriptivo y explicativo. Además, como instrumentos, se utilizaron documentos y una entrevista semiestructurada. Por su parte, se indagó sobre la aplicación del análisis operativo de casos a esta tipología delictual por parte del Poder Judicial de Córdoba. Además, se establecieron los casos más resonantes ocurridos en Córdoba en los últimos diez años, y se delimitó la diferencia entre ciberdelito y cibercrimen de la conducta ransomware. Entre los resultados, se halla una coincidencia de factores y conductas entre casos y una gran influencia contextual de la situación en cuanto a seguridad informática en los organismos, en la capacidad de reacción de estos. A su vez, no se encontró información que evidencie que el análisis operativo de casos se haya usado para estos delitos en la provincia de Córdoba. Por lo que se abrieron puertas a nuevas líneas de investigación y la creación de nuevas metodologías de abordaje gubernamental. Surgiendo como principal recomendación, la creación de un método de análisis de casos específico para el estudio de la conducta de cibercriminales y sus víctimas, con el fin de identificar las raíces causales del fenómeno y desarrollar así, políticas gubernamentales más eficaces para su prevención y control.

Palabras clave: Cibercrimen; Ransomware; Cifrado; Ciberataque; Hacker; Malware;Soft ware; TIC; Ciberespacio; Cibercriminal.

INTRODUCTION

The analysis of criminal behavior was constructed based on various contributions made by criminology and the behavioral sciences applied to the field of criminalistics practice.

The use of psychology to understand and prevent criminality must be considered from the origins of psychological science. However, the use and construction of methodologies with an empirical foundation are relatively recent.

The construction of psychological profiles was mainly based on the consideration, use, and development of classifications specific to psychiatry, which ended up pigeonholing offenders into possible diagnoses of mental illnesses. Over time, different theories were developed that began to consider other types of factors beyond psychological ones and that are fundamental for a more precise and accurate approach to the profile of a criminal.

According to Chilo, the foundations of this discipline correspond to practices carried out in the United States, in which the psychodiagnostic process is inverted and the result of the behaviors and actions of one unknown person is studied to deduce the type of subject who could have carried out the criminal act under investigation. In this way, data are collected and evaluated; the situation is reconstructed; hypotheses are formulated; the profile is developed and tested; and, finally, the results are reported.

The following can be cited as background:

- In 1943, the United States Secret Service asked psychiatrist Walter Langer to construct a psychological profile of Adolf Hitler. Langer had to predict the possible decisions Hitler would make if he were defeated. Of 8 alternatives proposed, Langer concluded that Hitler would opt for suicide.
- In 1957, Jambes Brussel constructed the first criminal psychological profile considered strictly as such. By comparing criminal behaviors with mental illnesses and taking into account crime scenes, he managed, through a deductive method, to delimit a profile whose statements corresponded with those of the Mad Bomber, an individual who planted numerous bombs in New York in the 50s.
- Since 1970, the FBI's contributions to the development of this technique were numerous. They create the Behavioral Science Unit. Robert Ressler, an FBI agent, creates the Criminal Personality Research Project, from which the patterns of conduct and behavior of murderers began to be documented. Among its most important contributions is the consideration of criminal seriality.

As this discipline begins to expand, multiple methodologies, developments, and conceptual definitions begin to emerge. Ressler considers the contributions made from the United States and points out that criminal profiling has been described as a sum of clues, as an attempt to gather specific information, and as a biographical sketch of behavioral patterns.

Holmes and Holmes consider three main objectives that emerge from the analysis and psychological study of the offender:

1. Approach to an assessment from social and psychological criminology of the offender's personality.
2. Consideration of the possible inferences regarding the offender's belongings found at the various crime scenes.
3. To lay the foundations for possible lines of inquiry and key hypotheses in criminal investigation.

In this context, therefore, criminal profiling seeks to generate an approximation of the characteristics of the alleged offender, which makes it possible to narrow the scope of the investigation and focus on more accurate and defined aspects. This is of great importance, considering that, as these are violent crimes and, above all, serial murders, social mobilization is high, since it must also be taken into account that the probabilities of a new crime being committed require interventions to be rapid.

This technique can feasibly be applied especially in cases in which seriality exists, since repetition makes it possible to determine the presence or absence of a pattern or behavioral pattern, especially in the crimes of rape, homicide, murder, and pyromania.

In Europe, the German school had the greatest influence on the determination of operational case analysis. It was used as an inductive method in the study of the information provided by the different branches of physical and natural sciences concerning criminalistics and through the objectivity of the evidence obtained by analyzing the behavior of an offender throughout the entire criminal act, considering its different phases, and by comparison with other criminal acts.

According to Fortete, criminal analysis involves methodically analyzing the criminal information that reaches the different operational areas and, thanks to citizen reporting, it is possible to

determine the sociopolitical, demographic, and criminal conditions that characterize a region or to use them for the resolution of specific cases.

On the other hand, it is essential to emphasize that the construction of a profile should not be limited solely to psychological considerations. Nor should the construction of that profile be taken as something rigid and immutable, given that the various analyses have shown that different profiles can emerge from a single situation or that the same profile can be modified due to the offender's refinement in their criminal career.

The methodology for constructing a criminal profile consists of analyzing and evaluating different aspects:

- The crime scene is the place and space that the offender has chosen to commit a crime. Scenes may be different if the offender uses and moves through various locations, that is, from the moment they capture their victim until they abandon them. In any case, the main scene is where the death or the most significant assault takes place. In this sense, the care and preservation of said scene are of fundamental importance, since each trace and clue can be key in determining a type of personality, while also considering the existence or absence of possible manipulations of said scene.
- The modus operandi refers to the method or way of operating.

It considers, primarily, the manner or method that the offender has used to commit the crime. From its analysis, information is gathered about how that criminal acts, which makes it possible to delimit and approximate the psychological characteristics inferable from his or her way of acting.

- The detailed study of the information provided by the modus operandi of offenders makes it possible to define indicators, such as the time of day chosen; the presence or absence of perfectionism; the manner of approaching the victim; whether or not there is planning and organization; the time spent; the intellectual level; the weapons; among others.
- The signature, for Robert Keppel, constitutes a part of the crime scene that involves different expressions of the criminal's fantasies, that is, it is the set of actions that are not necessary to commit the crime. The signature tends to be among the main patterns that make possible the establishment of seriality across different events, making it possible to attribute these to a sole perpetrator.
- The analysis of serial crimes is complemented by geographic analysis. There are various theories that explain the spatial behavior of the perpetrator of an act with the aim of establishing whether or not a relationship exists between these places and the routines of the offender. This profile describes the spatial conduct and the areas where the offender moves, the crime scenes, the anchor points of the events, risk zones, base of operations, etc.

We are living in an era where ICTs (information and communication technologies), electronic devices, social media, communication media and other services and products which are used to satisfy what we call "21st century needs"; we find that in addition to being used by the average citizen and companies, they are also used by States, governments, municipalities and government agencies for different purposes that can range from security, management of central banks (economic capital), provision of basic services for citizens (energy, water, gas, among others), educational systems, penitentiary systems and others where these technologies are present on a daily basis to facilitate processes or activities.

Nobody escapes the reality that ICT encompasses those elements and systems globally used today for the processing, exchange, and communication of information in today's society, and many are unaware of the extent to which these illegal activities known as cybercrime impact our society.

All technology that was developed from the 60s and 70s, with the arrival of the internet, underwent an expansionism and universalization of networks in which all people with access to an electronic device and the internet are directly and indirectly part of THE largest and most widespread communication network throughout the world, also called "the network of networks" Internet. Any person today who has a smart device, such as computers, cell phones, televisions, and a wide variety of appliances such as printers in offices, is connected to the internet.

As a consequence of such a milestone, it not only improved people's quality of life from entertainment to work and including medicine, but also provided tools to those people with "deviant behaviors" and opened a range of possibilities for those who, with knowledge and expertise in the use of computing, technology, and social engineering, knew how to use it for personal purposes and obtain those goods or objectives of value under a new modality of crime, a modality that spread by violating various rights such as sexual integrity, property, and liberty, crimes such as extortion, fraud, deception, and attacks on multinational banks or government organizations.

In many cases, these technologies are indispensable for carrying out work, facilitating it, and constituting a fundamental or critical part of it, where computers, mobile phones, files stored in

the cloud, programs/software, bank accounts, artificial intelligence, among others, are used. Any failure or intervention by any entity could paralyze the activities of the organizations that use them, producing problems depending on the time during which services are paralyzed, information is stolen, exposed, or damaged; the request for ransom for such information, page, or account is a frequent practice carried out by criminals. The effects of these failures or interventions, produced in the field of ICT and primarily through the use of these for their commission, are reflected in the citizenry and in its quality of life depending on the sector and group affected.

Cybercrime or computer crime, as it is known, is the name given to this "no longer so new" modality of crime; as generations passed and as technology evolved, so did its conception and meaning. According to Gustavo Sain (1), cybercrimes or computer crimes are considered to be any illegal conduct in which a computer device intervenes, whether as a means to commit the crime or as the end thereof. The first case contemplates cases of extortion or blackmail or intimidation via email, with the computer device being the object or target; and in the second case, the computer device is the target of the crime, where the person sends a virus to another person's device, damaging it or altering its operation.

The same was also done for the techniques of their commission or modus operandi (cybercrime) and for their diversification in terms of crimes, with examples such as white-collar crimes, phishing, malware, child grooming, dissemination of child pornography, fraud, identity theft, among others.

Although the variety of crimes that can be committed using ICTs is extensive, this document will focus on the commission of attacks on state and private organizations using ransomware or malicious software.

Ransomware is formed from the combination of the English words ransom (rescue) and ware (software); a ransomware attack can take many forms, including any type of malicious code or malware (in English), such as viruses, trojans, and computer worms. The propagation methods used are spam, vulnerabilities or poor software configurations, fake software updates, untrusted software download channels, and unofficial program activation tools.(2,3,4) The objective?

It is carried out through infection by destructive viruses, which in turn must be considered a typology of the more general behavior of malware or malicious software distribution intended to damage, control, or modify a computer system.

In cases where it is possible to encrypt, control, and deny the victim access to the information, the offender will request a ransom for that information, in some cases specifying how and in what currency payment should be made—for example, ransom in bitcoins or any other currency with blockchain technology—since this currency allows anonymity and is an asset that many entrepreneurs usually hold.

Ransomware is probably among the most serious cyber threats that private and governmental organizations can encounter, not only because of the damage it causes but also because cybercriminals constantly refine malicious code, making it harder to stop or detect, and because they constantly innovate to ensure ransom payment, increasing pressure on the victim by threatening them with everything they could do with their information.

In recent years, a transition has been observed in ransomware attacks, as they have moved from mass attacks (targeting a large number of people and demanding modest ransom amounts) to attacks targeting specific sectors, demanding much larger amounts from smaller groups of victims. These selected victims have greater financial resources, and their members cannot afford to lose access to or control of their data.(5)

To gauge how deeply ransomware attacks affect victims both technically and psychologically, it is necessary to know that there are different types, such as locking, denial of service (such as DDoS), and encryption types; it is easy to infer from the names what each of these types can do, but it is not very simple to predict the effects they leave on their victims.

Beyond the technical difficulties that cybercriminals leave in their wake after an attack are the "residual viruses" on devices or their mere presence in cyberspace, causing shock, as in the case of print bombing, which consists of infecting and using printers available on the target network to print messages demanding the ransom.

The enactment of Law 26.388(3), known as "the computer crime law," passed in 2008, introduced new criminal offenses related to the use of technology. Among all the new criminal offenses and articles added by this law is article 10, incorporated by said law, which punishes the alteration, destruction, or disabling of data, documents, programs, or computer systems, or the sale, distribution, circulation, or introduction into a computer system of any program intended to cause damage. This article and the characteristics of the conduct it describes correspond to those found in ransomware-type computer crimes.

One example of how the offender adapts to changes in order to commit crime can be seen in this "new" type of crime, computer crime; some opt for this path while others choose "conventional" crime, such as robbery with or without violence. This is seen from a general perspective and taking into account generational change and the evolution of technologies. But what if, in a particular case, the offender cannot commit conventional crime because he is confined at home like the rest of the citizens?

This situation occurred during the COVID-19 pandemic, when the entire Argentine population was forced to remain in quarantine at home due to the biological threat; in this situation, no person with active criminal activity could go out to carry out their activities without being detained by the authorities.

It is under these conditions that the offender, due to external factors, learns and adapts by using TIC as a new tool to commit crimes, taking advantage of the fact that a large part of the population used the internet. According to INDEC, for the last quarter of 2020, 86 % of the inhabitants of our country used the internet, which represents an increase of 5,6 percentage points compared to the previous year. According to the Management Report of the Unidad Fiscal Especializada en Ciberdelincuencia,(6) during 2019, a total of 2 369 reports were received, equivalent to approximately 6,5 reports per day without distinction between working days and non-working days, while for 2020, the number rose to 11 396, 381 % more, equivalent to around 31 reports per day. It is clarified that these data were taken using the population of CABA as a sample.

Among the modalities that occurred most frequently during that period are online fraud, unauthorized dissemination of images, harassment, and ransomware.

The Ransomware attack on Telecom Argentina on July 18, 2020. (7) This attack occurred globally, the 0-day ransomware based on the Sodinokibi malware. It is told 0-day if a hacker manages to breach the security before software developers can find a solution to that security vulnerability.

In this case, the problem was detected in time and affected only 5% of the company's computer equipment; neither the services nor the company's databases were affected, nor was any corporate client affected.

An example of what happens when a ransom is not paid for a ransomware attack and at the same time the affected organization is a government organization, on August 27, 2020 the National Directorate of Migration reported that it was the victim of a ransomware attack, losing data and this resulting in encryption, the gang called "Netwalkers" demanded the payment of the ransom for four million dollars.

On the day of the attack, various border points reported system problems. To preserve the data and assess the situation, the deactivation of SICAM (Sistema Integral de Captura Migratoria) was requested; the 5 land border crossings were closed, along with the Ezeiza and Buquebus airports, and for 4 hours there were no migratory movements as a result of the deactivation of SICAM.

The attack had repercussions because it was unusual for an attack of these characteristics to paralyze the activities of an entire country; it resulted in the resignation of the Director of Migration Systems, who had held the position for 2 decades at that time, and in the initiation of judicial proceedings. Amid this, cybercriminals set a deadline for payment of the ransom for the hijacked data; the state refused, which resulted in the publication of all the data.

What did the folders contain? According to Clarin, "Information from 2015 and 2016 linked to criminal intelligence, linked to security issues, Interpol cards or alerts."

The attack on the legislative body of the Senate at the beginning of 2022, also being a case of ransomware that blocked access to senators, restricting personal emails and paralyzing its functions.

Another case occurred approximately in the middle of 2022, in Córdoba: a ransomware attack on the judiciary that caused the outage of its services, paralyzing the activities of this body due to users' inability to access electronic records, official emails, temporary use of the physical case file, and with the risk of sensitive data being leaked.(8)

In this case, the incident occurred on October 9, 2021, when the Argentine state was the victim of a hack of the private database of individuals (Renaper), a database that contains all the private records of the country's inhabitants. Document numbers, addresses, transaction numbers (which are used for online credits), dates of birth, and, in some cases, cell phone numbers were leaked (2021).

The study of these crimes entails linking multiple factors, from the individual or collective practice of these crimes and their modes to the social-political-economic context of the victim(s) (which is political in cases where the entire country is affected or a large number of people and personalities are affected).

For the purposes of this manuscript, it is important to contextualize the issue of cyberattacks

in private and governmental organizations, situating ourselves in the Province of Córdoba and in its cases, approach, interventions, and studies on the topic. Therefore, the aim will be to determine governmental actions aimed at addressing the analysis of behavior.

Therefore, the general objective of this study will be:

- To describe and make explicit government actions in the criminal analysis of ransomware cybercrimes carried out by the Superior Court of Justice of the Province of Córdoba.

On the other hand, the specific objectives are:

- Investigate the possible implementation of operational case analysis in ransomware cybercrimes in the event that it has been implemented.
- Specify emblematic cases of ransomware cybercrimes in the province of Córdoba.
- Develop and specify modalities of cyber offenses and cybercrimes and their differences.
- Identify and specify modus operandi, signatures, and patterns of cybercrimes to provide an approach to criminal profiling.
- To examine in greater depth the actions of the local Justice system regarding ransomware-type cybercrimes.

METHODS

Design

For this research, a descriptive and explanatory investigation was conducted. This is because it seeks to describe how the behaviors, situations, and events caused by ransomware attacks occurred and manifested themselves in Argentina in general, and to explain them specifically in the province of Córdoba, in order to describe variables, phenomena, contexts, and cases for understanding the phenomenon.

The chosen approach is qualitative, meaning that there will be no measurements or numerical analyses or statistical analyses, only documentary sources and data collection. The objective is not to refute or test hypotheses.

Finally, it will be non-experimental in type, since there was no deliberate manipulation of variables, observing the facts just as they are presented for analysis.

Unit of analysis

The unit of analysis is documentary sources. These sources are of different types, such as journalistic articles and reports, academic papers, and testimonies in legal cases, among others. The selection of cases is justified by criminal and geographic characteristics in accordance with the proposed research topic.

Instruments

To achieve the stated objectives, the instruments used were documentary in nature; therefore, written sources and previously conducted and published interviews were consulted to corroborate the data on the phenomena.

Data Analysis

This section will provide definitions of fundamental terms and concepts for understanding the subject under discussion. With regard to the work plan, 3 stages are distinguished: The first stage consisted of a bibliographic analysis for the elaboration and construction of the theoretical framework. In the second, a documentary-type data survey was proposed. A collection, selection, and analysis of documentary sources were carried out according to the proposed objectives, such as academic papers, reports from official sources (governmental and non-governmental), jurisprudential sources, interviews, laws, and books, among others.

The third stage focused on the analysis of the data obtained, carried out with a qualitative approach, as well as their systematization according to the stated objectives, and the analysis and description of the information collected from the developed reference framework.

The data analysis was structured around the creation of categories, which are:

- Cybercrime: It is any unlawful conduct whose mode of action is carried out through electronic devices and social networks or cyberspace, with technology being the fundamental component of this “new” criminal process.
- Cybercrime: Modus operandi in the commission of a crime using mainly ICT.

- Ransomware: It is a type of malware or malicious software developed to lock the device and encrypt its data in order to demand a ransom for the subsequent restoration of the data and the re-enabling of the equipment.(1)
- Operational case analysis: This is the analysis of the structure, nature, and characteristics of cases to develop a profile of perpetrators, assess risks, compare cases, investigate their causes, and analyze the influence of social and cultural context.
- Social engineering: These are various manipulation techniques used by cybercriminals, who pose as another person with the aim of appropriating valuable data such as passwords or accounts.
- TIC: Information and communication technologies, as the name indicates, are technologies required for and used in the management and transformation of information. They include, in particular, computers and programs that enable the organization, storage, modification, and protection of information.
- Legal framework: The legal framework is the set of laws, rules, and regulations on which this document will be based, specifically Law 26.388 and, more specifically, Article 10 of this law.(3)
- Hacker: A person with computer knowledge who is dedicated or obsessed with finding flaws in organizations' computer security.
- Cyberspace: cyberspace, or the virtual world, is not a physical space in which any person can communicate and share through the media that allow access to it; these are the so-called TIC. Álvaro Écija (9) states, "it is already the fifth strategic environment, after land, sea, air, and space".

RESULTS

To investigate the possible implementation of operational case analysis in ransomware cybercrimes in cases in which it has been implemented:

No sources were found that affirm that the method of operational analysis of cases has been implemented in the province of Córdoba to analyze cyberattacks with the use of ransomware methodology. According to the data collected, it was concluded that the method allows its application to the criminal typology studied, since the authors are known for constantly looking for vulnerability in computer security systems or human error through the use of social engineering in organizations, although they can be innovative when it comes to changing the strategy or the malicious code once they were rejected, they will use the same technique until it is no longer useful and since they are not different in many of the cases there is the characteristic of seriality, as he stated in a particular interview made by Todo Noticia (10) to an expert in cybersecurity, where he says "they are of a common type, wild, there are criminals who scan thousands of servers per day and when they find a vulnerability they obviously attack it".

To identify emblematic cases of ransomware cybercrimes in the province of Córdoba.

Cases of cyberattack against organizations, whether public or private, tend not to be widely publicized. This is due in part to the fact that, unlike in other countries, there are no regulations on cyberattack reporting, or because, for reasons of impact and other issues, they are not made public; for example, a company called Globant publicly disclosed an attack it suffered and its shares fell 13 % on Wall Street. Accordingly, companies try to prevent this type of information from becoming public; the same applies to governments that suffer such attacks, as they seek to maintain control and prevent the affected population from panicking.

Even so, there is one emblematic case mentioned above that occurred in the province of Córdoba, although it is presumed that there are more and that they occur daily, which happened in the middle of the year 2022. This attack paralyzed judicial activities for a certain period; several emails were intercepted and there was a risk that the backup or backup copy would be lost; it forced the electronic file to be replaced by the physical file; and it affected about 8 000 users and nearly 25 thousand lawyers registered in the province.

In an interview with a cybersecurity expert conducted by a local channel from Córdoba, the expert stated: "Normally, this type of action is carried out by groups that seek to generate some panic in society".

Develop and explicitly state the modalities of cyberoffenses and cybercrimes and their difference.

Cybercrimes include the activities of cybercriminals, generic and low-severity activities, causing minimal harm to the civilian population, affecting one single individual or a group in the community. Some of these behaviors are computer fraud, forgery, scamming, extortion, harassment, grooming, offenses against intellectual property, hacking, corruption of minors, crimes against morality and decency, distribution of illegal content, and human trafficking. All these modalities, except for some, do not require prior experience in the use of ICTs and usually use common communication media such as WhatsApp, Facebook, or email for their commission; other techniques use social engineering and deception to obtain what they seek. The target is always the average citizen, who falls either due to ignorance or opportunism.(11,12)

Cybercrime is a more serious level within computer crimes, originating from cyberterrorists; their method of operation is through communication technologies to intimidate, harass, or coerce social groups in order to cause harm, all with political-religious purposes and/or acquisitive aims.(13)

Both phenomena exhibit similar characteristics in their respective techniques for breaching the security of computer systems, although they pursue different aims.

Identify and specify the modus operandi, signatures, and patterns of ransomware cybercrimes.

When considering computer crimes and their modes of operation, we find a large number of signatures and patterns that are left or demonstrated in the commission of cybercrime, all within the aforementioned ICTs. However, in cases of ransomware attacks, these modes, signatures, and patterns are visible in the different modalities that criminals use to deceive victims. Emails, messages, and computer worms, among other methods, are used in cyberattacks to compromise security, subsequently access and encrypt data, and then demand ransom, sometimes seeking the security of a currency or asset that is difficult to trace, such as cryptocurrencies (14,15).

At least the pattern seems clear: it is a sequential and methodical violation followed by theft and encryption, then proceeding to the demand, and, if the demand is not fulfilled, punishment.

The signature appears to be easy to obtain, since many cybercriminal gangs choose to display the name of the group in some way, although the same group could operate under many names, or a single malware could do so, and vice versa.

To further examine the actions of the local justice system regarding cybercrimes

The judiciary must opt to strengthen the actions of the specialized prosecutor's office for cybercrime by training specialized personnel in the prevention or detection of ransomware attacks, reinforcing its own infrastructure (since they have been targets of attack) and its security systems (because they have been bypassed on certain occasions), and training existing personnel to act post-incident, ruling out ransom payment or leaving it as a last resort, since there will be an upward trend in these crimes; options to consider could include the use of analog devices or a local connection system to safeguard information in closed circles of computers without connecting to the network, preventing access by third parties, with only authorized personnel handling those computers.

Do not leave everything completely automated, because that is what they seek: when a device is infected, its connection to the entire network will produce a contagion effect, spreading to other computers. The population must be adequately educated, with priority given to the adult population, since most of them are in a vulnerable position due to the poor adaptability that some have to new technologies, which makes them easily manipulated.

DISCUSSION

The research showed that the Argentine government and, by extension, the government of Córdoba, as well as the inhabitants, know little about the risks and consequences produced by the advancement of information and communication technologies, making them more vulnerable or prone to becoming victims of any type of crime that can be committed through these tools. If we analyze how the organizations or individuals who perpetrate this type of activity operate, we can observe that they persistently seek a vulnerability, distraction, or slip on the part of the victim or victims; they can be considered opportunistic or insistent depending on the cybercrime observed; they seek errors and take advantage of their victims' ignorance, and this is among the areas in which justice could act to strengthen and prevent the citizenry and its own agencies from suffering

hacks or breaches in their systems or networks. Throughout the research, the problem statement and the objectives changed; the available information on antecedents related to the province of Córdoba is scarce, and a mixed problem statement was sought, that is, to reveal antecedents from all or other parts of Argentine territory in addition to Córdoba.(16)

Among the limitations of this work was the limited background regarding the city of Córdoba; this paper is considered an additional and necessary contribution to the criminal analysis of these behaviors and to understanding the motivations behind these individuals, who seek opportunity, satisfaction, money, among others. A line of follow-up could be not to remain solely within the realm of cyberspace,

CONCLUSIONS

The objective of this research was to describe and make explicit the government actions that address the analysis of cybercriminal behavior related to ransomware carried out by the Superior Court of Justice of the Province of Córdoba. It should be mentioned that in the documentary sources consulted to answer this research question, it was possible to find evidence that allows us to infer that criminal behavior analysis can be used to analyze cases presenting these specific characteristics. However, no previous research was found that analyzes the casuistry of such events from the perspective of operational case analysis. These types of analysis are possible because they meet the essential characteristics they must have to be addressed by that method: seriality and unknown author(s). Although its scope is descriptive and explanatory, it constitutes a highly necessary contribution to the growth of the study, knowledge of the subject, and the construction of possible lines of research and also of new methods of criminal analysis, since it brings together the variables of attacks focused on the province of Córdoba in order to link them specifically with the operational case analysis method, which provides a novel answer to the main questions that constitute the essence of the manuscript. Among the social and cultural factors that influence the behavior of cybercriminals, the results found relate mainly to the structure of cyberspace and how criminals interact with it, which demonstrates how they adapt and learn to use that knowledge to commit crimes. The humiliations and degradations suffered by victims in the process demonstrate the vulnerability and the limited response they are left with after the attack, highlighting the impunity and freedom with which cybercriminals operate. Although the state has control of the media or at least telematic media, it is impossible for it to control the traffic and volume of information that exists, and prevention through awareness-raising is difficult for it.

REFERENCES

1. Sain G. Cibercrimen y delitos informáticos. Buenos Aires: Instituto de Pensamiento Penal; 2018. Disponible en: https://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf
2. Abogacía Española. Ransomware: una guía de aproximación para el empresario. Madrid: Consejo General de la Abogacía Española; s. f. Disponible en: https://www.abogacia.es/wp-content/uploads/2017/07/Guia_Ransomware.pdf
3. Ministerio de Justicia y Derechos Humanos. Ley 26.388. Delitos informáticos. Buenos Aires: Infoleg; 2008 jun 4. Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm
4. Moreno J, Rodríguez C, Leguias I. Revisión sobre propagación de ransomware en sistemas operativos Windows. 2019 mar 26. Disponible en: http://portal.amelica.org/ameli/jatsRepo/339/3391488005/3391488005.pdf
5. Secretaría de Innovación Tecnológica del Sector Público. El ransomware: el software malicioso usado para atacar a las organizaciones. Buenos Aires: Presidencia de la Nación Argentina; s. f. Disponible en: https://www.argentina.gob.ar/sites/default/files/2022/08/el_ransomware_el_software_malicioso_usado_para_atacar_a_las_organizaciones.pdf
6. Dirección Nacional de Ciberseguridad. Informe anual de incidentes de seguridad informática registrados en el 2021 por el CERT. Buenos Aires: Presidencia de la Nación Argentina; 2022 feb. Disponible en: https://www.argentina.gob.ar/sites/default/files/2022/02/informe_2_cert_2021_f_.pdf
7. Telecom Argentina. Información de Telecom sobre situación de ciberseguridad. Buenos Aires: Telecom Argentina; 2022 jul 20. Disponible en: https://institucional.telecom.com.ar/prensa/noticias/nota/informacion-de-telecom-sobre-situacion-de-ciberseguridad/415
8. El Doce. Por el ciberataque, la Justicia restringió sus actividades para el resto de la semana [video]. Córdoba: El Doce; 2022 ago 12. Disponible en: https://www.youtube.com/watch?v=Lg4wEBio3ts
9. Écijale Á. El ciberespacio: un mundo sin ley. s. f. Disponible en: http://ciberderecho.com/El_ciberespacio_un_mundo_sin_ley.pdf
10. Todo Noticias. Senado hackeado: denuncian un ciberataque al cuerpo legislativo [video]. Córdoba: TN; 2022 feb 1. Disponible en: https://www.youtube.com/watch?v=tbt0bBGxhd8
11. Secretaría de Educación, Subsecretaría de Promoción de Igualdad y Calidad Educativa. Grooming. Córdoba: Gobierno de la Provincia de Córdoba; 2016. Disponible en: https://www.igualdadycalidadcba.gov.ar/SIPEC-CBA/publicaciones/2016-Docs/grooming%202016.pdf
12. Fusz LR. Los problemas de determinación del grooming [tesis de pregrado]. Córdoba (AR): Universidad Siglo 21; 2017.
13. Erreius. Cibercrimen y delitos informáticos. 2018. Disponible en: https://www.errepar.com/resources/descargacontenido/CIBERCRIMEN.PDF
14. Ucciferri L. La ciberseguridad en la era de la vigilancia masiva. Buenos Aires: Asociación por los Derechos Civiles; 2016. Disponible en: https://adc.org.ar/wp-content/uploads/2019/06/013-A-ciberseguridad-en-la-era-de-la-vigilancia-masiva-05-2016.pdf
15. González ML. La cibercriminalidad como instrumento para la expansión y empoderamiento del crimen organizado. 2017. Disponible en: http://www.seguridadinternacional.es/?q=es/content/la-cibercriminalidad-como-instrumento-para-la-expansi%C3%B3n-y-empoderamiento-del-crimen
16. Cybersecurity Hub. Los principales desafíos que enfrenta el sector de la ciberseguridad en Córdoba y la región. Córdoba: CorLab; s. f. Disponible en: https://corlab.cordoba.gob.ar/wp-content/uploads/2022/07/Publicacion-Ciberseguridad-Hub-vertical.pdf

FUNDING

None.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHORSHIP CONTRIBUTIONS

Conceptualization: Agustín Ramiro Manrique Aguad, María Belén Gauna.
Data curation: Agustín Ramiro Manrique Aguad, María Belén Gauna.
Formal analysis: Agustín Ramiro Manrique Aguad, María Belén Gauna.
Investigation: Agustín Ramiro Manrique Aguad, María Belén Gauna.
Methodology: Agustín Ramiro Manrique Aguad, María Belén Gauna.
Project administration: Agustín Ramiro Manrique Aguad, María Belén Gauna.
Software: Agustín Ramiro Manrique Aguad, María Belén Gauna.
Supervision: Agustín Ramiro Manrique Aguad, María Belén Gauna.
Validation: Agustín Ramiro Manrique Aguad, María Belén Gauna.
Visualization: Agustín Ramiro Manrique Aguad, María Belén Gauna.
Writing – original draft: Agustín Ramiro Manrique Aguad, María Belén Gauna.
Writing – review and editing: Agustín Ramiro Manrique Aguad, María Belén Gauna.