Specificity of Ransomware Investigation

Analytical Study in Light of the European Cybercrime Programmed 2022

Received:19/12/2024;**Accepted:** 18/05/2025

Mohamed Said BOUFLIH [1*], Abdeldjabar CHAIBI [2]

[1] *Applied Legal Studies Laboratory, University of Constantine 1, Algeria. email: mohamed-said.bouflih@doc.umc.edu.dz*
[2] *Contracts And Business law Laboratory, University of Constantine 1, Algeria. email: Chaibiabdeldjabar@umc.edu.dz*

Abstract

This research article deals with the topic of ransomware attacks that have recorded a significant increase during the COVID-19 pandemic due to the large technology and digital services companies allowing their employees to work from home using their personal computers and enabling them to use passwords to access internal networks to complete the tasks assigned to them, where the negligence of some employees enabled hackers and intruders to use malicious software to penetrate networks and access companies' data and successfully encrypt them and then demand a ransom later.

This study allows for a close look at the most important details of launching ransomware attacks, and the methods used to collect criminal money, then addressing the European Union's guidelines for law enforcement agencies (judges, investigators) in investigating and investigating ransomware attacks to identify the attackers and ensure their prosecution, by presenting a guide in late 2022.

Keywords

Ransomware attacks;
Crypto currencies;
Cyberspace;
Cyber attackers;
European Cybercrime Office.

خصوصية التحقيق في هجمات برامج الفدية(دراسة تحليلية على ضوء البرنامج الأوروبي لمكافحة الجريمة السيبرانية 2022)

ملخص

يتناول هذا المقال البحثي موضوع هجمات برامج الفدية التي سجلت ارتفاعا كبيرا وقت جائحة كورونا بسبب سماح كبرى شركات التكنولوجيا و الخدمات الرقمية لعمل موظفيها من منازلهم باستعمال أجهزتهم الحاسوبية الشخصية وتمكينهم من كلمات المرور للدخول الى الشبكات الداخلية لإنجاز المهام الموكلة اليهم، أين تسبب إهمال بعض الموظفين من تمكين المتسللين و المخترقين باستعمال برمجيات خبيثة من اختراق الشبكات و الوصول الى معطيات وبيانات الشركات و النجاح في تشفيرها ثم المطالبة بالفدية لاحقا.

تتيح هذه الدراسة التعرف عن كثب على أهم تفاصيل شن هجمات برامج الفدية، و الطرق المعتمدة في تحصيل الاموال الاجرامية، ثم التطرق لإرشادات الاتحاد الاوروبي لهيأت إنفاذ القانون (قضاة، محققين) في التحري و التحقيق في هجمات برماج الفدية لتحديد هويات المهاجمين و ضمان محاكمتهم، من خلال طرح دليل أواخر سنة 2022.

الكلمات المفتاحية

هجمات برامج الفدية؛
العملات الرقمية؛
الفضاء السيبراني؛
المهاجمين السيبرانيين؛
المكتب الاوروبي للجريمة الالكترونية.

* *Corresponding author.E-mail: mohamed-said.bouflih@doc.umc.edu.dz*

Doi: https://doi.org/10.34174/0079-036-002-020

Introduction :

Modern digital technology has fundamentally transformed communication processes and service delivery, propelling the world toward unprecedented levels of efficiency and precision. This transformation has effectively collapsed spatial and temporal barriers with remarkable ease.However, this digital revolution has been accompanied by significant cybersecurity challenges, primarily manifesting as intrusions and cyberattacks targeting digital information and data flowing through cyberspace—data essential for delivering critical services.

The beneficial applications of technology have been paralleled by malicious uses that manifest in various forms and are driven by diverse motives—ranging from unethical and extremist purposes to the pursuit of illicit financial gains.Ransomware attacks constitute a significant form of cybercrime focused on financial extortion. Since the onset of the COVID-19 pandemic in early 2020, these attacks have evolved beyond targeting major global corporations and financial institutions, expanding to encompass medical services, healthcare facilities, and even small-scale individual enterprises.This situation has necessitated immediate and effective intervention by law enforcement authorities to address this escalating threat. Consequently, the institutions of the European Union (EU) and the Council of Europe have undertaken proactive measures to assist in investigations, enforce legal accountability against ransomware perpetrators, and ensure their prosecution.

This research is motivated primarily by the need to examine the factors driving the increasing prevalence of ransomware attacks at the international level—a trend that prompted the European Union to develop comprehensive guidance for law enforcement agencies in late 2022. This guidance aims to assist in investigating ransomware attacks and ensuring legal accountability, while our study seeks to elucidate the legal and technical dimensions of these attacks.

This study specifically excludes cases of cyber extortion where victims are blackmailed with threats of data leakage following a successful breach. Instead, it focuses exclusively on attacks utilizing malicious software designed to encrypt and render data inaccessible until a ransom payment is made.

The study analyzes the guidance document issued on December 8, 2022, in Bucharest, Romania, by the Council of Europe's Cybercrime Programme Office (C-PROC). The document provides a framework for criminal investigations into ransomware attacks under the European Union's Cybercrime Program (Sud-Cyber).

The key research question of this study is as follows:

How are ransomware attacks executed, and second, what procedural measures have been adopted by the European Union—through its specialized institutions, the Budapest Convention and its Second Additional Protocol, and member states' domestic laws—to ensure effective law enforcement and successful prosecution of perpetrators?

This research employs a multi-methodological approach:

1. A primary analytical methodology examining the recently issued guidance document

2. A descriptive approach investigating the nature of ransomware attacks, attack vectors targeting electronic devices, and ransom collection mechanisms

3. An inferential analysis of the regulatory framework established by the guidance document, the 2001 Budapest Convention, and its Second Additional Protocol, while considering individual privacy protections under member states' domestic laws

The subject will be addressed through two main sections. The first section provides a general overview of ransomware attacks, their legal and technical frameworks, and related contextual details. The second section examines the investigation methods and procedures proposed in the guidance document, aimed at assisting investigators and prosecutors in enforcing the law in ransomware cases to identify perpetrators and ensure their prosecution.

Section One: Introduction to the Concept of Ransomware Attacks

As is widely recognized, cyber-attacks represent a form of cyber threat that has become a significant source of danger in cyberspace and the internet world. According to the Tallinn Manual, cyber-attacks are defined as: "Those cyber operations, whether defensive or offensive, that are reasonably expected to cause injury or death to persons, or damage or destruction to objects (i.e., targets)"[1].

This definition reflects the broad scope of cyber-attacks and their potential to cause significant harm, emphasizing their critical impact on both the physical and digital realms.

Ransomware attacks represent one of the most prevalent forms of cyber-attacks, as a substantial segment of computer criminals, hackers, and cybercriminal groups primarily aim to achieve illicit financial gains through their activities. Ransomware attacks are particularly effective in this regard, as targeted victims—whether individuals, companies, or governments—often comply with ransom demands to regain access to their encrypted data and operational digital systems due to their critical dependence on these resources.

This type of cybercrime first emerged in 1989 through the actions of Joseph L. Popp, an American biologist from Harvard University. Popp distributed floppy disks (DISQUETTE) containing AIDS-related surveys with hidden malicious software. The concealed program, known as the "AIDS Trojan," caused operational difficulties on infected computers, ultimately encrypting data and making it inaccessible until a payment of $189 was sent to a designated post office box in Panama.

This scheme was implemented through the distribution of infected disks in a campaign falsely associated with the World Health Organization under the United Nations[2].

First: Definition of Ransomware Attacks

Ransomware is defined as "a type of malicious software from the family of encrypted viruses that threatens to publish victims' personal data, permanently block access to it, or sell it on the dark web unless a ransom is paid"[3].

It is also described as "malicious software that locks victims' computers or prevents access to data using private key encryption until the required ransom is paid, typically in Bitcoin"[4].

Advanced ransomware employs sophisticated techniques including crypto-viral extortion and social engineering. This software encrypts victims' files, making them inaccessible, and demands a ransom for decryption. Payments are typically made using cryptocurrencies such as PaysafeCard or Bitcoin, which are difficult to trace due to the algorithmic nature of their transaction protocols**[5].**

Ransomware is a form of malware that takes control of system data, making it inaccessible to users, systems, and applications. It operates on an extortion model: once the data is encrypted, a notification (through a readme file or remote screen) is typically sent demanding payment in exchange for data release**[6].**

It is noteworthy that ransomware attacks initially constituted only a small fraction of malicious software. However, in recent years, particularly since 2013, they have come to dominate the malware landscape, with Western Europe and North America becoming the regions most targeted by ransomware attacks**[7].**

Second: Types of Ransomware Attacks

Ransomware attacks vary in their forms based on the malicious software used, intended targets, and impact on encrypted data or systems. These attacks can be categorized into several types:

1. Locker Ransomware (File Locking Ransomware)

This type of ransomware blocks access to target computer systems and electronic devices, completely preventing the victim from using the device. The most common techniques employed in these attacks include social engineering and exploiting compromised system login credentials. The malware blocks system access until ransom payment[8], displaying a window on the targeted device's screen containing messages and images indicating encryption, such as:"Your computer has been used to visit illegal websites. To unlock your computer, you must pay a fine of $100."or"Your computer has been infected with a virus. Click here to resolve the issue"[9].

This type of malware was particularly prevalent between 2011 and 2012, with Reveton Ransomware being one of the most notorious examples[10]. This malware impersonated law enforcement authorities (judicial and security agencies) by executing drive-load attacks. Upon successful infection, it would display a message on the victim's screen falsely accusing them of crimes like "software piracy" or "accessing pornographic content online," demanding a monetary fine for future payment to unlock the device[11].

2. Crypto Ransomware (Encrypted File Ransomware)

This type of ransomware attack is the most prevalent, primarily aiming to encrypt important victim data such as documents, images, videos, and backup files, while leaving the core functionalities of the infected computer intact. Victims can identify the targeted files but cannot access them without paying a ransom in exchange for decryption keys that are sent later.

The widespread nature of crypto ransomware can be attributed to internet users neglect of backing up personal data to external storage devices or utilizing individual storage and cloud services available through specialized information storage companies such as Google Drive, Amazon, Dropbox, and others.

Malware developers enhance these programs with additional features, including countdown timers for ransom payment deadlines, specified payment methods, and other relevant details[12].

3. Ransomware as a Service (RaaS)

In recent years, ransomware has become highly profitable, emerging as an available digital service (commodity) where producers offer various types to potential customers through the dark web. Several platforms specializing in this criminal service have emerged, including Satan, Cerber, Hostman, Flux, and Atom[13].

These platforms allow criminals to easily launch ransomware attacks without needing to develop the malware themselves, thus broadening the accessibility of such attacks to a wider range of cybercriminals.

This type of software provides criminal digital services by enabling individuals interested in launching ransomware attacks—whether beginners or those lacking advanced programming skills—to use ready-made malware in exchange for commissions offered in various forms.These financial gains take multiple forms, including selling malicious software through the dark web to buyers or receiving percentage-based commissions from successful attacks on targeted victims[14].

This method allows specialized criminal groups and ransomware developers to reduce the risk of identity exposure and remain beyond the reach of regulatory authorities.Malicious ransomware services are marketed online, with over 6,000 websites selling ransomware products and services, offering more than 45,000 viral programs for initiating ransomware attacks.

These sites provide various ready-to-use malicious ransomware packages with prices ranging from $20 to $3,000 for premium offerings[15].

The operational process with RaaS providers involves potential attackers creating an account on the portal, paying using digital currencies, and requesting desired malicious programs. Criminal proceeds are shared between program users and service providers at varying rates, typically ranging from 50% to 80% of collected revenues.

4. Double Extortion Ransomware

In this type of attack, cybercriminals extract sensitive digital data from targeted electronic devices in addition to encrypting it. This approach provides attackers with additional leverage points to compel victims to pay the demanded ransom amounts[16].

The methodology of double extortion ransomware operates as follows: Once attackers gain network access, they map the targeted network, identify sensitive data, extract it, and then execute the ransomware attack. If victims refuse to pay the demanded ransom, the malware operators threaten to auction the extracted data on specialized sites for sale, thus generating funds equivalent to the demanded ransom amount[17].

Third: Impact of Ransomware Attacks and Recovery Methods

The impact of successful ransomware attacks varies in severity, ranging from minor system and data encryption to severe cases where data recovery becomes impossible. The severity largely depends on the specific malicious software used in the attack and whether the attack occurred in an online or offline environment (Online/Offline).

1 - Impact of Ransomware Attacks

Ransomware attacks have generated multiple risks for individuals, businesses, governments, and both traditional and digital services, including:

- **Financial Risks:** These encompass ransom payments, data recovery expenses, legal fees, and regulatory fines, resulting in substantial financial losses for targeted victims. Additionally, encryption can severely damage the victim's reputation, leading to further financial strain.

- **Operational Risks**: Infected systems and compromised data can cause operational disruptions, resulting in work stoppages, appointment cancellations, and potential employee layoffs. These disruptions affect not only daily operations but also long-term organizational functionality.

- **Legal Risks:** Data breaches and insufficient security incident responses expose organizations to legal consequences, including compensation lawsuits and significant financial penalties. These arise from failures to protect sensitive data and maintain compliance with data protection regulations.

- **Reputational Risks:** The credibility of targeted victims, particularly legal entities, suffers as stakeholders—including business partners, existing clients, and potential customers—question the security of their IT infrastructure and business operations.

- **Personal Risks:** Attacks may target sensitive personal data, including academic research, thesis work, and personal files, potentially causing professional, psychological, or emotional distress. This can extend to identity theft and unauthorized disclosure of personal information.

- **Security Risks:** These attacks can significantly impact healthcare services and critical infrastructure, affecting the ability to use medical equipment for treatment and potentially endangering lives. These vulnerabilities pose serious risks not only to individuals but to entire communities, particularly when essential services are compromised[18].

2 – Data and Operating System Recovery Methods in Ransomware Attacks

When a system is infected by ransomware, whether online or offline, access to encrypted data or systems becomes impossible. The challenge is particularly acute when victims lack backup copies of the affected data.

Data recovery can be attempted through two main approaches:

Paying the Attackers: The first recorded ransom demand in 1989 requested $189 to be sent to a postal account in Panama[19].

This method proved costly and impractical. The process evolved as attackers shifted to using email, attaching "read me" files with encrypted data that contained payment instructions, including method, location, and required payment means. Between 2008 and 2009, a new development emerged: antivirus software containing Trojan horse ransomware that utilized security programs like Pro Fix File to collect payments[20]. The introduction of cryptocurrencies later significantly streamlined ransom collection due to their inherent features, particularly the extreme difficulty in tracing transaction paths and origins.

It is crucial to note that paying criminals does not guarantee the recovery of encrypted systems and data. Security agencies, legal authorities, and cybersecurity service providers strongly advise against this solution, as it facilitates the proliferation of these attacks and encourages criminals to continue their illegal activities.

Using Recovery Software: Various products are available in the cybersecurity space, complemented by technical support from major global information security companies.

For example, companies like Kaspersky (with its “No Ransom” initiative[21]) occasionally offer free or low-cost solutions to victims of ransomware attacks.

These tools help in recovering encrypted files and systems by following guidelines provided by these companies.They assist in identifying the malware used in the attack and provide decryption tools where possible.

Section Two:Mechanisms for Investigating Ransomware Attacks According to the European Guide for Cybercrime Investigations

Investigation comprises a set of legal and technical procedures conducted by competent authorities, involving crime scene examination, analysis of available evidence, and proper assessment of facts, all while respecting fundamental freedoms and adhering to public authority constraints and procedures in accordance with the principle of procedural legality.

The unique nature of ransomware attack investigations lies in achieving the desired balance between investigative effectiveness and protecting individual and collective rights and freedoms, particularly the right to privacy. Additionally, these investigations must respect procedural legitimacy and the admissibility of electronic evidence[22].

The European Cybercrime Investigations Guide provides detailed instructions on:

- Collecting Digital Evidence: This includes advanced techniques for handling encrypted data, monitoring affected systems, and analysing digital logs.

- International Cooperation: Since many ransomware attacks occur across borders, the guide includes guidance on cooperating with international law enforcement bodies like Europol or Interpol.

- Modern Technologies: Investigations into ransomware attacks often require advanced analysis tools to detect malicious software and decrypt files, as well as building investigators' capacity to manage digital evidence effectively.

In conclusion, the goal of investigating ransomware attacks is to identify the perpetrators and protect the affected data and systems while maintaining respect for individuals' rights and privacy.

This can be achieved by following precise legal procedures that ensure the admissibility of evidence in court and uphold justice in investigations.

The Budapest Convention on Cybercrime, specifically in Chapter 1, Section 1, mandates that treaty parties must adopt all necessary legislative measures to investigate crimes specified within the convention[23].

Given the escalating threat of ransomware attacks, it has become imperative to assist law enforcement authorities in investigating these incidents, considering both their unique characteristics that distinguish them from other cybercrimes and the sophisticated technical capabilities of cybercriminals. Investigators, prosecutors, and judges need clear guidance on required procedures to ensure effective combat against these attacks and successful prosecution of perpetrators.

To enhance investigative effectiveness in ransomware cases, the competent authorities in the European Union and Council of Europe have introduced a "guidance manual"[24]proposing procedural rules to assist law enforcement, including methods for collecting electronic evidence and ensuring access to perpetrators.

The objective of this manual, which is the subject of this study, is to provide law enforcement personnel and judicial practitioners with guidance on conducting criminal investigations into ransomware attack cases.

This manual serves as a complement to a series of training programs, workshops, reports, guides, and other supporting tools developed by the Council of Europe to support the fight against all forms of cybercrime.

Several other related guides complement the ransomware investigation guidelines, including:

- Guide on Electronic Evidence (released in 2022).
- Guide on Seizing Crypto currencies.
- Guide on Initial Responders in Cybercrime Investigations (released in 2021).
- Judicial Guide for Judges and Prosecutors (prepared in 2018)[25].

Additionally, there are other materials and training courses relevant to the issue, such as:

- International Law Enforcement Training Course on Ransomware Investigations (2022).

- Judicial Specialized Training on International Cooperation (2021).
- Judicial Training on Financial Investigations, Virtual Currencies, and the Dark Web[26].

It is important to note that this guideline focuses on the specific aspects of ransomware investigations, without addressing the legal or procedural rules related to how investigations, questioning, or prosecution procedures should be conducted before the relevant judicial authorities. These matters fall under the procedural rules of the national laws of each state party to the Convention on Cybercrime or its second additional protocol.

Therefore, this guideline primarily aims to:

- Understand the specific characteristics of investigating ransomware attacks.
- Outline the steps involved in investigating ransomware attacks.
- Provide methods for international cooperation in investigating ransomware attacks.

This approach helps ensure that investigators and legal professionals are equipped with the necessary tools and knowledge to effectively combat ransomware, while respecting the legal frameworks and privacy rights of individuals[27].

The Cybercrime Convention Committee (T-CY) of the Council of Europe has adopted a guidance note on ransomware.

This note explicitly states that ransomware attacks are criminal acts that must be criminalized and punished[28].

Ransomware attacks constitute one of the criminal behaviors outlined in the Cybercrime Convention.

The convention identifies various forms that malicious software used in ransomware attacks can take For example:

- The malicious software used in ransomware attacks may involve unauthorized access to the victim's computer systems, which is covered under Article 2 of the convention.
- The software may also aim to intercept data transfers between computers and information systems, which is prohibited under Article 3 of the convention, titled "Illegal Interception of Data".
- In some ransomware attacks, malicious software seeks to manipulate digital data from the targeted computers and take control of them, which is addressed and prohibited under Article 4 of the convention.
- Article 5 of the convention further criminalizes actions that interfere with the functioning of computer systems in order to gain control over them.

The subsequent articles of the convention criminalize the production of ransomware, including acts like selling, buying, importing, distributing, or displaying such software, or creating fraudulent digital data for phishing purposes. This also extends to offenses committed by legal entities (corporations, organizations, etc)[29].

As a result, committing these acts requires strict intervention by the domestic laws of the countries that are parties to the Cybercrime Convention.

These laws should include deterrent penalties such as imprisonment and, when necessary, additional sanctions.

This ensures that ransomware attacks are met with a firm legal response and deterrence, safeguarding the integrity of digital systems and protecting individuals and organizations from the damage caused by such cybercrimes.

In the investigation of ransomware attacks, it is essential to follow the legal steps required for this type of crime, based on the rules established in the Cybercrime Convention and its Second Additional Protocol, while also adhering to the domestic laws of each country. This must be done in a way that respects the right to privacy. The investigation process primarily focuses on several key steps.

First: Digital Forensic Evidence

Digital forensic evidence refers to material or immaterial facts that can help uncover the crime, clarify uncertainties, or prove the accuracy of the facts being investigated. These types of evidence are essential for investigators and judges to base their findings and judgments on[30].

However, handling electronic evidence requires attention to thespecific nature of this evidence. Digital evidence is not tangible; it is typically in the form of binarycode(0s and 1s), which is perceptible only through specialized electronic devices, such as computers or specificsoftware. It serves as a scientific tool for reconstructing the crime, helping investigators trace the incident to identify the offender, the victim, or the crimescene[31].

1. Guidelines for Collecting Digital Forensic Evidence

When collecting digital forensic evidence related to ransomware attacks, it is important to follow the internal laws governing criminal activities. These laws should be enforced during the collection of electronic evidence from ransomware incidents and considered as proof before law enforcement authorities[32].

Key recommendations for handling digital evidence include:

- **Immediate preservation**: The first step is to use legal powers to secureandpreserve the compromised data on the infected computer, especially information related to the source or distributionpath of the malicious software. This may involve identifying where the ransomware originated, how it spread, and any communication that occurred regarding the ransom demand.

- **Evidence related to ransom demands**: Collecting records of any communication between the attacker and the victim, such as emails, chat logs, or instructions about the ransom payment. This will help in tracking the attacker's activity and possibly identifying patterns or connections between different attacks.

- **Decryption tools**: Evidence of any tools offered by the attacker for decryption or payment instructions related to the ransom demand should also be captured. These tools may serve as crucial elements in tracing the hacker's methods and infrastructure.

By following these guidelines, investigators can ensure that **digital evidence** is properly handled, documented, and preserved, enabling effective legal action and the prosecution of those responsible for ransomware attacks[33].

2. Securing Electronic Evidence

When a victim reports a ransomware attack, beforeanyclean up or data recovery activities take place, it is crucial for investigators to secure the compromised data. The steps involved include:

- **Scope of the Attack**: Investigators should quickly assess the scope and size of the ransomware attack, identifying the affected systems, network infrastructure, and files.

- **Identification of Malicious Software**: Determining the exact type of malware used in the attack is essential. Tools such as Kaspersky No RansomandNo More Ransom[34] can help identify the ransomware variant and assist in potential decryption efforts.

By securing the compromised devices early, investigators can preserve critical evidence such as malicious software, encryption keys, and attack traces that are vital for the investigation.

3. Analysing Malware

To conduct a successful forensic investigation, understanding the nature of the malware used in the ransomware attack is critical. Ransomware can vary in functionality, including:

- **Encrypting Files**: Some ransomware simply encrypts files, making them inaccessible.

- **Changing File Types**: Other types may change the file format, rendering the data unusable unless decrypted.

- **Encrypting Backups**: Some sophisticated ransomware variants also target backup files, making recovery more difficult[35].

Investigators can request limited information from email service providers to track the communication between the attacker and the victim, particularly messages that contain the ransom instructions. These may include wallet addresses for crypto currency payments, which could be linked to the attacker's financial transactions.

4. Financial Investigation

A significant aspect of ransomware attacks involves the use of crypto currencies for ransom payments. Despite crypto currencies being decentralized, they rely on block chaintechnology which provides a permanent ledger of transactions[36].

Investigators can leverage tools like chainalogy[37], Graph Sense[38], bitcoinwhoswho[39], localbitcoins[40]and others to trace crypto currency transactions. These tools allow for the tracking of transactions through blockchain analysis, identifying the flow of funds and potentially linking them to known cybercriminalnetworks.

In addition, the KnowYourCustomer **(KYC)[41]** protocols used by many crypto currency exchanges provide another avenue for law enforcement to gather information about the entities involved in the transactions. By linking digital wallets to real-world identities, investigators can uncover the true identities of the individuals behind the ransomware attacks.

By following these investigative steps, authorities can not only track the perpetrators of ransomware attacks but also build a case to prevent future attacks and bring those responsible to justice.

5. Open Source Investigation

Open Source Intelligence (OSINT) relies heavily on analysing publicly available data to trace cybercriminals involved in ransomware attacks. This process includes studying both previous and new identities of cybercriminals, especially those who change their online personas after engaging in ransomware activities. Investigators and law enforcement agencies must meticulously search for critical information[42], such as:

- Usernames, email addresses, and IP protocols
- Crypto currency wallet addresses used for ransom payments
- Phone numbers, passwords, and images tied to the cybercriminals
- Programming techniquesanddevelopment languages used in the malware code

By focusing on these data points, investigators can uncover the true identities of attackers and track their activities through the open web, dark web, and other platforms. OSINT also enables the study of malware programming techniques, which can aid in identifying specific malware strains used in the ransomware attack.

Tools for Open Source Investigation in Ransomware CasesOne popular open-source tool for criminal investigations is **Maltego**[43], which can assist investigators in mapping out connections between various digital identities and ransomware activities.

- **Maltego** allows investigators to: Integrate with various open-source databases such as:
  - **Pipl Database[44]**: Helps link online identities with real-world individuals.
  - **Leaked Password Database[45]**: Useful for finding links to compromised credentials and malicious activities.
  - **Spider Foot[46]**: An OSINT tool that aggregates data from different sources to reveal hidden digital footprints.
  - **X Intelligence[47]**: Provides insight into metadata and online behavior that can help identify links between ransomware actors and their networks.
  - **Majestic[48]**: Offers data on web footprints and helps trace relationships between online entities.
- **Visualization and Link Analysis**: **Maltego** offers graphical link analysis to illustrate connections between people, transactions, and digital actions. These visual diagrams make it easier for investigators to understand how ransomware groups and their affiliates are connected.

How OSINT Enhances Ransomware Investigations

- **Tracing Digital Footprints**: OSINT enables investigators to track digital activities such as **email exchanges**, **crypto currency transactions**, and **IP addresses** involved in ransom payments. These details provide key leads that can eventually lead to identifying suspects or tracing the payment route.

- **Malware Analysis**: Investigators can also analyse the **malware code** and the **programming languages** used in ransomware to find similarities with other known cybercriminal groups or techniques, helping to link ransomware strains to specific hacker communities.

- **Uncovering Hidden Identities**: OSINT tools like Maltego can be used to search for **previous usernames**, email addresses, and other identifiers that may have been used by the attackers before they created new, hidden identities. This makes it possible to reveal **cybercriminals' past activities**, even if they have taken steps to cover their tracks.

By leveraging OSINT techniques, law enforcement can gather invaluable data to support investigations into ransomware attacks. This approach allows for tracing financial transactions, uncovering hidden digital identities, and building a clearer picture of how ransomware campaigns are organized and executed.

Second: Cooperation in Combatting Ransomware Attacks

Ransomware attacks involve various stakeholders, including attackers, targeted victims, digital service providers, financial institutions, social media platforms, and expanding jurisdictions. As a result, effective international cooperation is crucial for investigating and collecting electronic evidence in ransomware attacks.

Given the urgent need to strengthen cooperation in combating cybercrime, the **Budapest Convention on Cybercrime(2001)anditsSecond Additional Protocol** (May 2022) significantly enhance international collaboration and evidence collection, including between public and private sectors[49].

1. Requesting Assistance from Digital Service Providers (Judicial Assistance)

A successful investigation into ransomware attacks often requires the joint effort of various digital service providers[50]. These include:

- **Internet Service Providers (ISPs)**: They play a crucial role in identifying internet traffic associated with the attack.

- **Email Service Providers**: They can provide valuable evidence, such as email correspondence between the attacker and the victim.

- **Hosting Service Providers**: These are critical for tracing malicious infrastructure used in the attack.

- **Social Media Platforms**: They are often used for communication between cybercriminals and victims or for tracking ransomware extortion demands.

- **Crypto currency Exchange Platforms**: As ransomware attacks often involve crypto currency payments, exchanges are crucial for tracking financial transactions related to the ransom.

Digital service providers are tasked with monitoring content, identifying domain names[51], and assisting with identifying suspicious activities. International cooperation in this area is supported by mechanisms outlined in the Budapest Convention, particularly in requesting judicial assistance across borders.

2. Sirius Project

The Sirius Project aims to assist investigators in overcoming the complexities involved in cybercrimes, including ransomware attacks. It specifically addresses the vast amount of data in cyberspace and the challenges investigators face in collecting relevant information.

- The Sirius Project provides guidance on how to obtain specific types of data and offers detailed steps to access information from 60+ online service providers.

- It facilitates collaboration through a platform operated by the European Union Agency for Cyber security **(ENISA)**, where experts from EU countries and partner countries can exchange best practices and experiences in investigating cybercrime.

The project is designed to enhance the ability of investigators to navigate the challenges posed by the massive volume of data involved in digital evidence collection and to ensure that law enforcement agencies have the tools they need to fight cybercrime, including ransomware.

Through these initiatives, international cooperation in addressing ransomware is significantly improved, ensuring that law enforcement and investigators have the resources, legal frameworks, and support from the private sector necessary to address these complex and evolving cyber threats.

This project is a collaborative initiative between the European Union Agency for Law Enforcement Cooperation (Europol)**,** theEuropean Union Agency for Criminal Justice Cooperation (Eurojust), and the European Judicial Network (EJN). It offers targeted guidance to law enforcement authorities and judicial officials tasked with investigating ransomware attacks.

The Sirius Project provides tools and instructions to assist in:

- Accessing and interpreting data from major service providers.
- Facilitating collaboration between EU member states and countries with agreements on data-sharing and cybercrime investigation.
- Enabling smoother coordination between judicial authorities and law enforcement for better handling of electronic evidence[52].

3. International Cooperation Rules Under the Budapest Convention (2001)

The Budapest Convention on Cybercrime outlines several mechanisms to facilitate international cooperation in investigating and prosecuting ransomware attacks. Key features include:

- Sharing of Investigation Outcomes: Article 26 allows the sharing of information and results from investigations related to ransomware attacks without requiring formal assistance requests or prior approval[53].
- Evidence Collection: Articles 23 to 28 focus on international cooperation for collecting electronic evidence in ransomware attacks. This includes mechanisms for cross-border data preservation, access to stored data, and legal assistance in criminal investigations.
- Operational Provisions: Articles 29 to 35 detail additional international cooperation measures, such as expedited extradition requests, access to real-time data, and joint investigative efforts[54].

4. Enhanced Cooperation Rules in the Second Additional Protocol (2022)

The Second Additional Protocol to the Budapest Convention introduces significant updates to strengthen international collaboration for ransomware investigations. These updates include:

- **Access** to Subscriber Information: Streamlined procedures for obtaining subscriber data and identifying attackers through digital service providers.
- Urgent Data Disclosure: New provisions for the immediate disclosure of stored data during emergencies to prevent further damage or escalation of ransomware attacks.
- Video Conferencing and Joint Investigation Teams: Facilitating cross-border collaboration through video conferencing for interviews, hearings, and evidence collection. It also formalizes the establishment of JointInvestigation Teams (JITs) for coordinated efforts.
- Privacy and Personal Data Protection: Article 13 of the Protocol ensures that all cooperation respects privacy rights and personal freedoms. This includes safeguards against misuse of data and adherence to privacy standards in international data-sharing agreements.

- Accelerated sharing of critical data for real-time investigations.
- Strengthened collaboration between law enforcement and private sector entities, such as digital service providers and crypto currency platforms.
- Clearer procedural guarantees to balance effective law enforcement with respect for fundamental rights.

These collaborative frameworks significantly bolster the ability of countries to respond to ransomware threats while safeguarding individual rights and maintaining the integrity of international cooperation[55].

Conclusion

This research paper has addressed a highly significant and contemporary topic concerning law enforcement and the unique legal and technical challenges involved in investigating cybercrimes, particularly ransomware attacks, which have proliferated in recent years. The study focused on analyzing the aforementioned guidance document and its implementation.

Through this research, we have conducted a detailed examination of ransomware attacks, their execution methods, and the most commonly employed malicious software. We traced the temporal evolution of financial revenue collection methods for retrieving encrypted digital systems and data through ransom payments. The study highlighted the unfortunate role of cryptocurrencies and their various features that have facilitated the alarming growth of this criminal activity in recent years. This escalating threat necessitated urgent intervention, leading the European Union, through its specialized institutions, to develop a guidance manual to assist law enforcement authorities in investigating ransomware attacks. This guidance aligns with the 2001 Budapest Convention on Cybercrime and its Second Additional Protocol regarding enhanced cooperation and electronic evidence disclosure, while respecting fundamental rights and freedoms, particularly digital privacy rights as established in member states' domestic laws.

Findings

This research has revealed:

- Limited Law Enforcement Capabilities: Law enforcement agencies face significant constraints in technical resources and capabilities when addressing ransomware attack challenges.
- Insufficient Coordination: There is inadequate coordination among enforcement agencies, authorities, and private sector entities in combating these attacks.
- Legislative Gaps: Many jurisdictions lack explicit domestic legislation criminalizing ransomware attacks.
- RaaS Proliferation: The unchecked growth of Ransomware-as-a-Service (RaaS) models on the dark web continues unabated.

Recommendations

Based on our findings, we recommend:

- Criminalization of Ransom Payments: Following Algeria's approach to criminalizing traditional ransom payments to terrorist groups, ransomware payments should be similarly criminalized.
- Third Additional Protocol: Developing a third additional protocol to the 2001 Budapest Convention specifically addressing ransomware attacks.
- EU Open-Source Platform: Establishing an official European Union open-source platform to assist ransomware attack victims in recovering their data and operational systems free of charge.
- These recommendations aim to enhance the effectiveness of counter-ransomware efforts while maintaining an appropriate balance between security measures and privacy protection.

Referrals and References

First/ Sources

- Budapest Convention on Cybercrime, Council Of Europe (RAMANIA) 23 November 2001.
- Second Additional Protocol To The Convention On Cybercrime On Enhanced co-operation And Disclosure Of Electric Evidence, Council Of Europe Treaty Series No. 224, Strasbourg 12 May 2022.
- The guide to conducting criminal investigations into ransomware attacks, which is the subject of this study, was prepared by the Cybercrime Office C_PROC with the contributions of: Alexander Catalin Kosi, Catalin Zito, Victor Voels, within the framework of the IPROCEEDS_2 project of the European Cybercrime Programme Cyber Sud, published in Bucharest on 8 December 2022 and is available on the website of the Cybercrime Section of the Council of Europe.
- Tallinn Manual on International Law Applicable to Cyber Warfare, prepared by a group of international experts at the invitation of NATO, Editor-in-Chief Michael N Schmitt, 2013, translated by Ali Muhammad Kazim Al-Moussawi, 2017, under the supervision of Prof. Dr. Haider Adham Al-Taie.
- Guidance Note No. 12 on T-CY Aspects of Ransomware Covered by the Budapest Convention, Report adopted on 30 November 2022, from the Report Series of the Committee on Cybercrime Convention.
- Cybercrime Convention Committee (T-CY), µT-CY Guidance Note #12 Aspects of ransomware covered by the Budapest Convention.

Second/ References

1 – Books

- Lahcen Nani, Investigation of crimes related to information technology between legislative texts and technical privacy, - New University Publishing.
- Hadda Boukhalfa, Criminal Liability of Internet Service Providers, Dar Houma for Printing, Publishing and Distribution, Algeria.

2 – Theses

- Raja Oumdour, The Privacy of Investigation in the Face of Cybercrimes, A Thesis for a Third-Level Doctorate in Private Law, Mohamed Bachir El Ibrahimi University, Bordj Bou Arreridj, Faculty of Law and Political Science - Department of Law - Academic Year 2020-2021.

3 – Academic articles

- Ben Alia Ben Jeddou, Abbas Darar, The Economic Effects of Electronic Crime, Journal of Contemporary Economic Research, Volume 5, Issue 1, Year of Publication 2022.
- Hamid Hashlafi, Cyber psychology as a diagnostic tool for cybercrime, hacking hospital data as a model for study, Algerian Journal of Human Security, July 2023.
- Kok SH, Abdullah Azween, Jhanjhi NZ, Mahadevan Supramaniam, Ransomware Threat and Detection Techniques: A Review, IJCSNS International Journal of Computer Science and Network Security, VOL.19 No.2, February 2019.
- Ronny Richardson, Max M North, Ransomware-Evolution Mitigation andPrevention, Kennesaw State University, Digital Commons Kennesaw State University, 01-01-2017.
- Jason E Thomas, Rayan P Galligher, Macalah L Thomas, Gordon C Galligher, Enterprise-Cyber security-Investigating-And-Detecting Ransomware infections using digital forensic techniques, published by Canadian center, 2019.
- Amin kharraz, techniques and solutions for addressing ransomware attacks a dissertation presented in partial fulfillment of the requirements for the degree of, college of computer and information science northeastern university.
- Fatimah Abdauiji, Omar Botarfi, Manal Bayousif, Utilizing-cyber-threat-hunting-techniques-to-find-ransomware attacks: a survey of the state of the art, 2022, this article has been accepted for publication in IEEE Access.
- Lily Hay Nemman, The Dangerous New Ransomware Trick Is Encrypting Your Data Twice, May 17, 2021.

4 – Online articles

- Protection against ransomware (The Zero Trust) Security Model for the Modern Workforce, Cisco Systems, Published 2021: https://www.cisco.com/c/dam/global/ar_ae/products/collateral/security/protect-against-ransomware.pdf.

5 – Websites

- What is ransomware, learn more about malware, how it works and how you can protect yourself and your business from it, ransomware protection, ransomware attacks in the news : https://www.microsoft.com/ar/security/business/security-101/what-is-ransomware#Ransomwaredefined.
- REVETOMRANSOMWARE, for lien : https://www.knowbe4.com/reveton-worm.
- Ransomware attacks create a range of risks to individuals, businesses, communities and critical services, from financial, operational, legal or professional risks to safety and security challenges, https://www.coe.int/en/web/ransomware/risks-and-challenges.
- Kaspersky threats, at the link :https://threats.kaspersky.com/en/threat./
- Training materials, guides, templates,https://www.coe.int/en/web/octopus/training.
- The online tools – Country Wiki profiles on cybercrime legislation and policies, training materials and many more to come – bring together experts, counterparts, academics and professionals in the cybercrime field, https://www.coe.int/en/web/octopus/home.
- NO MOR RANSOM, site web lien: https://www.nomoreransom.org/ar/ransomware-qa.html.
- Binance site officiel : https://www.binance.com/ar/price.
- **GraphSense** is a crypto asset analytics platform with an emphasis on full data sovereignty, algorithmic transparency, and scalability. GraphSense is open source and free. It provides a dashboard for interactive investigations and, more importantly, full data control for executing advanced analytics tasks, Site web lien: https://graphsense.info/.
- crypto and bockchain, Site web lien: https://ciphertrace.com/.
- Bitcoins Whos Who, Site web Lien: https://www.bitcoinwhoswho.com/.
- Local Bitcoins has been closed, Site web lien: https://localbitcoins.com/.
- REGULA, Site web lien: https://regulaforensics.com/ar/id-verification/.
- MALTEGO, investiqate 12 X faster with the words most used cyber investigation platform, Site web lien: https://www.maltego.Com/.
- nobody knows people like pipl, the 1 source for online identity and trust, Site web lien: https://pipl.com/.
- DEHASHED, take your personal security to the next level, Site web lien: https://dehashed.com/.
- INTEL471, attack surface protection, Site web lien: https://www.spiderfoot.
- Intelligence, Site web lien: https://intelx.io/.
- OSINT Framework, Site web lien: https://osintframework.com/.
- EUROPOL platform for experts, Site web : https://epe.europol.europa.eu/group/sirius.

References

[1]. Schmitt, M. N. (2013), Tallinn Manual on International Law Applicable to Cyber Warfare, NATO CCD COE, translated by Al-Moussawi, A. M. K. (2017), supervised by Al-Taie, H. A., pp.1-215.

[2]. Simone, A. (2017), The Strange History of Ransomware, The World, pp.1-8, Visited: 15/09/2024, https://theworld.org/stories/17/05/2017/ransomware-0.

[3]. Kok, S.H., Azween, A., Jhanjhi, N.Z., Supramaniam, M. (2019), Ransomware Threat and Detection Techniques: A Review, IJCSNS International Journal of Computer Science and Network Security, 19(2), pp.136-142.

[4]. Richardson, R., North, M. M. (2017), Ransomware-Evolution Mitigation and Prevention, Kennesaw State University Digital Commons, pp.1-15, Visited: 16/09/2024, https://digitalcommons.kennesaw.edu/facpubs.

[5]. Microsoft Security (2023), What is Ransomware? Learn More About Malware, Visited: 15/09/2024, https://www.microsoft.com/ar/security/business/security-101/what-is-ransomware#Ransomwaredefined.

[6]. Thomas, J.E., Galligher, R.P., Thomas, M.L., Galligher, G.C. (2019), Enterprise Cybersecurity: Investigating and Detecting Ransomware Infections Using Digital Forensic Techniques, Canadian Center of Science and Education, pp.73-82.

[7]. Hashlafi, H. (2023), Cyber Psychology as a Diagnostic Tool for Cybercrime: Hacking Hospital Data as a Model for Study, Algerian Journal of Human Security, July 2023, pp.251-26

[8]. Kharraz, A. (2020), Techniques and Solutions for Addressing Ransomware Attacks [Doctoral dissertation], College of Computer and Information Science, Northeastern University, pp.61-85.

[9]. Abdauiji, F., Botarfi, O., Bayousif, M. (2022), Utilizing Cyber Threat Hunting Techniques to Find Ransomware Attacks: A Survey of the State of the Art, IEEE Access, pp.5-20.

[10]. KnowBe4 (2023), Reveton Ransomware Analysis, Visited: 11/10/2024, https://www.knowbe4.com/reveton-worm.

[11]. Richardson, R., North, M. M. (2017), Ransomware-Evolution Mitigation and Prevention, Kennesaw State University Digital Commons, pp.10-15.

[12]. Cisco Systems (2021), Protection Against Ransomware: The Zero Trust Security Model for the Modern Workforce, pp.3-8, Visited: 13/10/2024, https://www.cisco.com/c/dam/global/ar_ae/products/collateral/security/protect-against-ransomware.pdf.

[13]. Thomas, J.E., Galligher, R.P., Thomas, M.L., Galligher, G.C. (2019), Enterprise Cybersecurity: Investigating and Detecting Ransomware Infections, Canadian Center of Science and Education, pp.74-82.

[14]. Cisco Systems (2021), Protection Against Ransomware, op. cit., pp.3.

[15]. Ben Jeddou, B.A., Darar, A. (2022), The Economic Effects of Electronic Crime, Journal of Contemporary Economic Research, 5(1), pp.570, Visited: 12/10/2024 (Written in Arabic).

[16]. Newman, L. H. (2021), Ransomware's Dangerous New Trick Is Double-Encrypting Your Data, WIRED, Visited: 15/12/2024, https://www.wired.com/story/ransomware-double-encryption/

[17]. Council of Europe (2023), Ransomware Risk Assessment Framework, Visited: 13/11/2024, https://www.coe.int/en/web/ransomware/risks-and-challenges.

[18]. Council of Europe (2023), Risks and Challenges - Ransomware, Visited: 15/11/2024, https://www.coe.int/en/web/ransomware/risks-and-challenges

[19]. Cisco Systems (2021), Protection Against Ransomware, op. cit., pp.4.

[20]. Cisco Systems (2021), Protection Against Ransomware, op. cit., pp.4.

[21]. Kaspersky (2023), Threat Intelligence Portal, Visited: 15/09/2024, https://threats.kaspersky.com/en/threat/

[22]. Oumdour, R. (2021), The Privacy of Investigation in the Face of Cybercrimes [Doctoral dissertation], Mohamed Bachir El Ibrahimi University, Faculty of Law and Political Science, pp.129.

[23]. Council of Europe (2001), Budapest Convention on Cybercrime, CETS No.185, Articles 2-12, Visited: 17/10/2024, https://www.coe.int/en/web/cybercrime/the-budapest-convention.

[24]. Council of Europe (2022), Guide to Conducting Criminal Investigations into Ransomware Attacks, C-PROC Bucharest, IPROCEEDS-2 Project, Visited: 12/11/2024, https://www.coe.int/en/web/octopus/training.

[25]. Council of Europe (2023), Training Materials and Templates, Octopus Project, Visited: 22/11/2024, https://www.coe.int/en/web/octopus/training.

[26]. Council of Europe (2023), Cybercrime Legislation and Policies Wiki, Visited: 21/11/2024, https://www.coe.int/en/web/octopus/home.

[27]. Cybercrime Convention Committee (2022), Guidance Note No. 12 on T-CY Aspects of Ransomware, Council of Europe, Visited: 15/12/2024, https://www.coe.int/en/web/cybercrime/-/ransomware-new-guidance-note-by-the-t-cy.

[28]. Cybercrime Convention Committee (2022), T-CY Guidance Note #12, op. cit.

[29]. Council of Europe (2001), Budapest Convention on Cybercrime, op. cit.

[30]. Oumdour, R. (2021), op. cit., pp.119.

[30]. Oumdour, R. (2021), op. cit., pp.119.

[32]. Council of Europe (2022), Guide to Conducting Criminal Investigations into Ransomware Attacks, op. cit., pp.18.

[33]. Nani, L. (2018), Protecting the Digital Economy between Criminal Policy and Digital Citizenship, Electronic Economy Journal, Istanbul Institute for Economic Studies and International Cooperation, 1(1), pp.125.

[34]. No More Ransom Project (2023), Ransomware Q&A Portal, Visited: 05/11/2024, https://www.nomoreransom.org/ar/ransomware-qa.html.

[35]. Council of Europe (2022), Guide to Conducting Criminal Investigations into Ransomware Attacks, op. cit., pp.21.

[36]. Binance (2023), Cryptocurrency Exchange Platform, Visited: 15/10/2024, https://www.binance.com/ar/price.

[37]. GraphSense (2023), Crypto Asset Analytics Platform, Visited: 22/09/2024, https://graphsense.info.

[38]. CipherTrace (2023), Cryptocurrency Intelligence Platform, Visited: 01/11/2024, https://ciphertrace.com.

[39]. Bitcoin Who's Who (2023), Bitcoin Address Lookup Service, Visited: 18/10/2024, https://www.bitcoinwhoswho.com.

[40]. LocalBitcoins (2023), Peer-to-Peer Trading Platform [Archived], Visited: 22/10/2024, https://localbitcoins.com.

[41]. Regula Forensics (2023), ID Verification Platform, Visited: 14/09/2024, https://regulaforensics.com/ar/id-verification.

[42]. Council of Europe (2022), Guide to Conducting Criminal Investigations into Ransomware Attacks, op. cit., pp.27.

[43]. Maltego Technologies (2023), Cyber Investigation Platform, Visited: 23/11/2024, https://www.maltego.com.

[44]. Pipl (2023), Identity Trust Platform, Visited: 14/10/2024, https://pipl.com.

[45]. DeHashed (2023), Security Intelligence Platform, Visited: 10/11/2024, https://dehashed.com.

[46]. SpiderFoot (2023), Attack Surface Protection Platform, Visited: 03/12/2024, https://www.spiderfoot.net.

[47]. IntelX (2023), Intelligence Platform, Visited: 23/11/2024, https://intelx.io.

[48]. OSINT Framework (2023), Open Source Intelligence Tools, Visited: 23/11/2024, https://osintframework.com.

[49]. Council of Europe (2022), Second Additional Protocol to the Convention on Cybercrime, CETS No.224, Strasbourg.

[50]. Boukhalfa, H. (2019), Criminal Liability of Internet Service Providers, Dar Houma Publishing, Algeria, pp.120.

[51]. Binance (2023), Cryptocurrency Exchange and Market Data Platform, Visited: 22/11/2024, https://www.binance.com/ar/price.

[52]. Europol (2023), SIRIUS Platform, Visited: 21/11/2024, https://epe.europol.europa.eu/group/sirius.

[53]. Council of Europe (2001), Budapest Convention on Cybercrime, op. cit.

[53]. Council of Europe (2001), Budapest Convention on Cybercrime, op. cit.

[55]. Council of Europe (2022), Second Additional Protocol to the Convention on Cybercrime, op. cit.