Framework for Monitoring Malicious Channels in Phishing Campaigns: A Cyber Threat Intelligence Perspective

Ivo Ricardo Dias Rosa
Invited Assistant Professor
ISTEC - Instituto Superior de Tecnologias Avançadas, Lisbon, Portugal
Email: ivorosa@gmail.com
ORCID: 0000-0002-9612-4491

Abstract: **Phishing campaigns are becoming more sophisticated, using encrypted communication platforms like telegram to coordinate their activities and store stolen information. This paper introduces a structured and scalable framework that supports cyber threat intelligence (CTI) efforts in monitoring malicious telegram channels linked to phishing activity.The framework is based on a combination of machine learning and human expertise, and it leverages a large dataset of telegram messages and their corresponding labels to train and evaluate the performance of the model. The methodology involves four interconnected stages: extracting hidden artifacts from phishing code, gaining unauthorized access to private telegram groups, analyzing collected data automatically, and implementing counterintelligence measures to prevent detection. Initial findings validate the framework's ability to detect indicators of compromise (IoCs) and visualize the attacker's infrastructure. Additional functionalities like integration with threat intelligence platforms and artificial intelligence-based data enrichment enhance the framework's versatility and usefulness. This method improves proactive communication monitoring, providing a secure and flexible solution for tracking adversarial communication channels.**

Keywords: **Cyber Threat Intelligence, Phishing Campaigns, Malicious Channel Monitoring, Telegram, Indicators of Compromise, Telegram Monitoring, Malicious Code Analysis**

I. INTRODUCTION

The field of cybersecurity is encountering increasing difficulties due to the rapid expansion of phishing campaigns, which utilize both social engineering tactics and technical weaknesses to gain unauthorized access to individuals and organizations [1].

Over the years, these campaigns have transformed from basic email scams to sophisticated operations that incorporate multiple layers of deception, automation, and decentralized coordination. One worrisome trend is the use of communication platforms like telegram, which offer attackers a secure, anonymous, and easily accessible space to handle stolen data, distribute harmful tools, and coordinate ongoing attacks.

These platforms are frequently utilized to host command-and-control (C2) infrastructures or serve as repositories for stolen credentials, documents, and configuration files. Telegram's encryption capabilities and its open API make it an appealing target for malicious activities, but also pose significant challenges for cybersecurity experts trying to monitor or prevent such actions. A frequently neglected but vital component in addressing these threats is the examination of malicious code deployed by attackers [2]. This code often includes important indicators like telegram bot tokens, api keys, and group or channel identifiers. When correctly extracted and analyzed, these artifacts can provide direct access to attacker-controlled environments and reveal valuable insights into their operational strategies.

Nevertheless, the process of infiltrating and monitoring these malicious channels is not a simple task. Threat actors frequently utilize defensive mechanisms, such as automated detection bots and manual vetting of new participants, to ensure operational security and prevent unknown observers from joining their activities. These counter-surveillance techniques greatly diminish the effectiveness of conventional intelligence gathering methods.

In order to tackle these difficulties, this paper suggests a framework specifically designed to identify, gain access to, and analyze malicious telegram channels in phishing scenarios. By integrating malicious code analysis, passive surveillance techniques, and cyber counterintelligence practices, the framework provides support to Cyber Threat Intelligence (CTI) teams in identifying indicators of compromise (IoCs) and obtaining valuable insights into attacker behavior and infrastructure.

Although telegram has become a popular tool for phishing attacks, most CTI frameworks lack comprehensive strategies for infiltrating and studying these malicious online environments. Existing research frequently examines these elements independently. This research addresses the lack of a comprehensive and practical approach for real-time threat monitoring, providing CTI teams with improved visibility into the communications of attackers.

II. STATE OF THE ART

In recent times, Cyber Threat Intelligence (CTI) has emphasized the importance of monitoring infrastructures that

are under the control of malicious actors, such as domains, command-and-control (C2) servers, and communication platforms. In this particular situation, the importance of messaging services, particularly those with robust privacy features, has increased substantially.

Among the various platforms, Telegram has gained popularity among cybercriminals due to its user-friendly interface, end-to-end encryption capabilities, ability to support large groups and channels, and relatively lenient terms of use. These qualities have made it a flexible tool for managing operations, spreading malware, and sharing stolen information [3].

Phishing Campaigns and Malicious code Infrastructure

Recent research has shown that phishing attacks are becoming more sophisticated, with cybercriminals using code to store or retrieve sensitive information like stolen credentials, access logs, and compromised endpoints [2]. Notably, many of these campaigns involve the use of pre-determined elements **(**hardcoded artifacts**)** like bot tokens, api keys, or direct links to telegram channels and groups within scripts or payloads [2, 4]. These hidden components not only assist the attackers in their operations but also provide avenues for defenders to identify and dismantle malicious infrastructures.

The connection between phishing techniques and messaging platforms presents a significant but understudied avenue for CTI initiatives [5]. By deconstructing phishing kits or payloads, researchers can frequently uncover identifiers that, when handled correctly, grant access to attacker-controlled telegram environments. These locations may hold a vast amount of threat intelligence, such as indicators of compromise (iocs), information about the victims, and evidence of a larger campaign's coordination.

Challenges in Monitoring Malicious Channels

Despite the potential value of such monitoring, several technical, operational, and legal obstacles persist. Among the most pressing challenges are:

- *Detection by adversaries:* Sophisticated threat actors frequently deploy automated bots and behavioral analytics tools to monitor the activity within their channels. These counter-surveillance measures can identify and remove unauthorized or suspicious participants, significantly limiting observational opportunities [6].

- *High data volume:* Malicious channels often operate with high message throughput, mixing relevant IoCs with noise, memes, or benign chatter. Filtering this information in real-time or near real-time presents a major analytical bottleneck.

- *Technical and legal constraints:* Platform-imposed limitations on API access, account creation, or automation may hinder the ability to collect and process data at scale. In addition, jurisdictional variations in privacy laws can restrict research activities or necessitate strict oversight [7].

Despite these barriers, sustained monitoring of malicious Telegram channels remains a critical component of modern CTI. It supports the identification of emerging threats, enables the discovery of IoCs, and contributes to a proactive cybersecurity posture capable of anticipating and neutralizing phishing operations before they escalate.

III. METHODOLOGY

In order to tackle the challenges associated with identifying, accessing, and analyzing malicious telegram channels utilized in phishing campaigns, this paper introduces a structured framework consisting of four sequential and interconnected phases. Each phase is designed to tackle distinct operational and technical challenges faced during Cyber Threat Intelligence (CTI) investigations, guaranteeing a systematic and consistent approach to intelligence collection.

3.1. Analysis of Phishing Campaign Code

The first stage of the project concentrates on gathering and examining code samples from ongoing phishing campaigns, without any active involvement. These samples may consist of various types of files, such as html templates, Javascript files, obfuscated scripts, or malware executables, which can contain valuable artifacts like:

- URLs pointing to malicious infrastructure (e.g., command-and-control servers),

- Telegram bot API tokens [8],

- Group or channel identifiers used for storing or distributing exfiltrated data [8].

Static analysis tools and custom scripts are employed to extract, parse, normalize and standardize these elements. The extracted artifacts are then structured and cataloged into a centralized repository to facilitate future cross-referencing and automated correlation with known threat indicators.

3.2. Access, monitoring tracking of Telegram Channels

After gathering telegram identifiers, the framework's second phase focuses on discreetly accessing malicious channels.

Due to the fact that numerous groups controlled by attackers are monitored by both automated bots and human operators for any suspicious behavior, it is crucial to conduct covert infiltration [9].

Strategies include:

- Creation of authentic-looking accounts that mimic regular user behavior and profile characteristics [3];

- Deployment of bots designed to simulate human-like interactions, including randomized message viewing patterns and realistic session durations;

Passive monitoring is carried out to reduce the chances of being detected, avoiding actions like replying to messages, reacting to comments, or downloading files that could alert adversary systems.

3.3. Examination of gathered information

After gaining access, the third phase concentrates on the automated extraction and analysis of pertinent information from the monitored channels. This includes:

- Parsing messages to identify Indicators of Compromise (IoCs), such as target email lists, stolen credentials, malware hashes, phishing URLs, and screenshots [2],
- Structuring and indexing the extracted data in searchable databases, enabling correlation across multiple campaigns and facilitating threat actor attribution.

Natural Language Processing (NLP) techniques can also be used to help with language normalization and entity recognition, particularly in situations where the language is multilingual or the code is difficult to understand.

3.4. Counterintelligence and detection avoidance

The last stage involves implementing counterintelligence strategies to guarantee extended, covert monitoring within environments controlled by the adversary. Techniques include:

- Account and IP rotation, using multiple identities and geographical proxies to distribute access patterns;
- Use of Virtual Private Networks (VPNs) and proxy chains to hide the origin of monitoring activity [6];
- Obfuscation of bot behavior to mimic organic user dynamics, including randomized delays, navigation patterns, and interaction limits.

Combined, these tactics allow the framework to maintain persistence in hostile environments while minimizing the operational footprint and reducing the likelihood of analyst attribution [10].

IV. PRELIMINARY RESULTS

While the complete execution of the proposed framework is still in progress, preliminary tests and controlled deployments have provided encouraging evidence that supports its viability and efficiency in various operational stages.

In the initial stages of analyzing phishing code, around 15% of the samples studied had hardcoded references to telegram groups, channels, or bot tokens [2]. These components were commonly found within phishing kits or malicious scripts that were used to process stolen data or establish communication with infrastructure controlled by attackers. This discovery strengthens the significance of telegram as a platform for coordinating threats and suggests that it should be a key focus in CTI operations.

During the channel access and monitoring phase, it was essential to utilize realistic and properly configured accounts, which included personalized bios, profile photos, activity history, and metadata that aligned with the region. Controlled experiments showed that these accounts were much less likely to be flagged or removed by automated detection bots or adversary administrators, especially when combined with behavior emulation techniques like randomized activity intervals and limited passive interaction [6].

Despite the limited scope of deployment, the framework proved effective in extracting crucial indicators of compromise (IoCs), such as phishing urls, email addresses of targeted victims, telegram handles of affiliated actors, and lists of harvested credentials. This intelligence has already played a role in identifying new attack patterns, such as previously unknown domains and the reuse of credentials across multiple campaigns. In certain instances, connections were made between phishing kits and operational telegram groups, allowing for the creation of threat actor profiles by analyzing communication patterns and shared resources [3].

These initial findings highlight the framework's ability to improve CTI capabilities by granting structured access to adversary communication environments, enriching threat datasets, and facilitating predictive analysis through continuous monitoring over time.

Drawing inspiration from current CTI practices, the proposed framework introduces a novel amalgamation of automated artifact extraction, human-behavioral emulation for covert access, and multi-layered data correlation across multiple campaigns.

Its flexible design enables easy integration with threat intelligence platforms and artificial intelligence modules, ensuring scalable monitoring capabilities.

It is crucial to highlight that this multi-phase approach is tailored for a particular threat landscape, specifically phishing campaigns that incorporate telegram as part of their operational infrastructure during their development cycle. In these situations, telegram serves not only as a means of communication, but also as a storage and distribution platform for stolen credentials, phishing kits, and coordination among malicious individuals.

Due to this limitation, the framework's applicability is restricted to situations where this architectural dependency is present. Numerous phishing campaigns still depend on traditional infrastructures like hacked websites, email gateways, or data drop zones, without integrating messaging platforms. This specificity inherently limits the ability to generalize the findings and compare them with broader trends in phishing attacks.

This specificity corresponds with research that telegram is gradually gaining popularity, but it is not yet the dominant method used in phishing ecosystems [11].

Despite the fact that only a few campaigns utilize telegram, this framework gives an edge in intelligence gathering by allowing continuous, covert access to environments controlled by adversaries. This feature provides valuable insights based on user behavior, which can be used in

conjunction with traditional ioc feeds to improve CTI response strategies. It offers a deeper understanding of the context and relevance of the information.

This section compares this approach to conventional CTI models, emphasizing its unique position and added value in specialized monitoring scenarios.

V. COMPARATIVE CONTEXT

Unlike conventional Cyber Threat Intelligence (CTI) methods that concentrate on domain names, phishing email headers, or static malware signatures, the proposed framework aims to address adversarial infrastructure on encrypted messaging platforms, which have become a significant vector in contemporary phishing attacks.

In contrast to conventional CTI systems that primarily rely on structured threat feeds like IP blacklists, domains, and URLs gathered from open-source intelligence (OSINT) and honeypots, these approaches often lack integration and behavioral context, which restricts their situational awareness [12-14]. Additionally, passive telemetry-based systems do not enable real-time observation of attacker tactics or communication dynamics, which limits the understanding and disruption of campaign coordination [15].

Recent academic suggestions have highlighted the importance of connecting threat data from both structured and unstructured sources to enhance the reliability of indicators of compromise (IoCs) [12]. This framework expands upon previous academic proposals that emphasize data correlation across CTI sources [16], by introducing a covert engagement layer focused on adversary-controlled messaging platforms. Nevertheless, these approaches primarily rely on aggregated data feeds and do not have direct access to communications between adversaries. The framework presented in this work takes the current state of the art to the next level by providing secure and long-lasting access to telegram channels controlled by attackers, shedding light on their campaign strategies, tool distribution, and behavior patterns in real-time.

In contrast to passive threat feeds, this approach yields actionable intelligence by continuously monitoring over time, thereby improving situational awareness and the predictive abilities of CTI analysts.

VI. CHALLENGES AND LIMITATIONS

Although the initial findings and the planned framework appear promising, its practical execution is fraught with significant challenges and limitations that need to be recognized and resolved to guarantee long-term operational effectiveness and ethical standards.

One of the main challenges is the ability of threat actors to quickly adapt their methods, tactics, and procedures (TTPs) in response to surveillance. As monitoring capabilities improve, attackers may abandon Telegram or adopt more obscure, decentralized, or encrypted platforms that offer increased resistance to infiltration and tracking [7].The use of encrypted messaging apps has become increasingly popular in recent years, as individuals seek to protect their privacy and secure their communications. This ongoing game of adaptation and evasion necessitates frequent updates to methodologies and swift intelligence cycles.

Legal and ethical concerns pose substantial obstacles, particularly when addressing private or exclusive communication platforms. Differences in data protection laws across jurisdictions, like the General Data Protection Regulation (GDPR) in the european union, can impose strict limitations on passive monitoring activities, especially when sensitive data belonging to individuals is at stake [4]. Researchers need to strike a balance between gathering intelligence and respecting privacy, making sure to follow legal guidelines and practicing responsible disclosure [17].

From a technical perspective, the creation, implementation, and upkeep of monitoring systems necessitate specialized knowledge in reverse engineering, automation, threat intelligence, and secure network operations. Furthermore, the necessity to replicate human actions, handle multiple accounts, and process extensive amounts of incoming data escalates operational complexity and resource utilization.

The issue of scalability persists, particularly as phishing campaigns expand across various languages, regions, and attack methods. Balancing monitoring efforts while maintaining secrecy and accuracy is challenging and may require the use of automation, artificial intelligence, and distributed architectures to remain efficient.

Despite these limitations, the framework still holds value. However, they emphasize the need for additional research, continuous refinement, and strategic collaborations, establishing the framework as a solid base for advancing CTI practices in a rapidly evolving threat environment.

VII. FUNCTIONAL EXTENSIONS OF THE PROPOSED FRAMEWORK

In addition to its main stages, the suggested framework can be expanded to include various functional enhancements that enhance its efficiency, scalability, and compatibility with other Cyber Threat Intelligence (CTI) and incident response systems. These improvements are particularly beneficial in fast-paced and resource-limited settings, where up-to-date and enriched intelligence can significantly impact strategic and tactical decision-making.

6.1. Integration with threat intelligence platforms

To make the most of the gathered data, the framework can be combined with well-known Threat Intelligence Platforms (TIPs), such as MISP (Malware Information Sharing Platform) and OpenCTI. These platforms facilitate the automatic collection and enhancement of IoCs obtained from malicious Telegram channels. By utilizing structured sharing through formats like STIX/TAXII, the intelligence can be compared with other datasets to identify patterns, shared infrastructure, and assess the capabilities of adversaries. This cooperative approach promotes interoperability, minimizes redundancy, and facilitates coordinated responses among reliable partners [18].

6.2. Evaluation of Our Risk and Threat Analysis Prioritization

A dynamic risk scoring system can be incorporated to evaluate and prioritize monitored channels based on multiple factors, such as message frequency, presence of sensitive content (e.g., credentials, internal documents), and indicators of technical sophistication (e.g., obfuscation techniques, use of automation or encryption). These scores provide support for contextual threat ranking, enabling analysts to prioritize the most significant threats and allocate resources effectively. This corresponds to established enterprise risk management frameworks and enables the integration of CTI outputs into broader organizational risk models [18].

6.3. Visualizations,operational and interactive dashboards

Sophisticated visualization tools and dashboards have the power to convert raw data into easily understandable and actionable insights. By utilizing temporal and spatial analyses like activity heatmaps, IoC frequency graphs, and channel-specific message volumes, analysts can quickly identify anomalies, changes in behavior, or coordinated activities. By implementing real-time alerts triggered by specific conditions (e.g., the rapid dissemination of credential lists or phishing kits), organizations can improve their situational awareness and take proactive measures. These interfaces are advantageous for both technical investigators and strategic decision-makers, as they bridge the gap between raw intelligence and its practical impact on operations [18].

6.4. Automation and Scalability with Artificial Intelligence

To tackle challenges related to volume, complexity, and timeliness, the framework can utilize artificial intelligence (AI) and machine learning (ML) capabilities. AI models can assist in automatically classifying messages based on established threat patterns or detecting anomalies, while ml algorithms can be trained to identify coordinated campaign behaviors by analyzing linguistic, structural, or temporal factors. NLP models enhance the framework by extracting entities, identifying threat actor aliases, and interpreting obfuscated messages or code snippets [19].

Crucially, incorporating Explainable AI (XAI) techniques guarantees that ai-driven insights remain transparent and auditable, fostering trust and empowering analysts to verify and substantiate automated decisions in critical investigative scenarios [18]. These AI-driven capabilities not only scale monitoring efforts effectively, but also enhance human expertise, resulting in a synergistic approach to CTI.

VIII. CONCLUSION AND FUTURE WORK

Keeping an eye on the channels used by malicious phishing campaigns provides a valuable perspective on the attackers' infrastructure, tactics, and operational patterns. With the growing prevalence of platforms like telegram among threat actors for storing stolen data, distributing phishing kits, or coordinating activities, the demand for effective, scalable, and covert monitoring solutions becomes increasingly urgent. This paper introduced a detailed framework that combines the analysis of malicious code, covert access to attacker-controlled channels, automated data processing, and cyber counterintelligence strategies to support Cyber Threat Intelligence (CTI) initiatives.

By utilizing static artifact extraction, discreet channel observation, and structured analysis of indicators of compromise (IoCs), the framework facilitates the early identification of adversarial behaviors, aids in strategic threat attribution, and assists in mitigating ongoing and future phishing campaigns. Additionally, the suggested functional enhancements, such as integrating threat intelligence platforms and implementing AI-powered automation, establish the framework as a versatile base for both operational and research-driven deployments.

Nevertheless, the ever-changing risk environment necessitates ongoing adjustment. Future work will therefore emphasize:

- Refinement of stealth monitoring techniques**,** including behavioral mimicry, advanced obfuscation, and adaptive identity management to avoid adversary detection;
- Incorporation of AI and machine learning models for large-scale data parsing, campaign pattern recognition, and predictive threat modeling;
- Collaborative engagement with communication platforms and policymakers to establish monitoring protocols that balance operational intelligence needs with ethical and legal standards [4].

In parallel, emphasis will be placed on developing explainable and auditable systems, ensuring transparency in automated processes and maintaining analyst trust in high-stakes CTI environments. Ultimately, the evolution of this framework will contribute to more proactive, intelligent, and resilient responses against phishing threats in an increasingly digital threat landscape.

REFERENCES

[1] M. Afonso and J. Santos, “Cyber Threat Intelligence: Técnicas de Monitorização em Plataformas Digitais,” *Journal of Cybersecurity Studies*, vol. 12, no. 3, pp. 45–58, 2023.
[2] P. Costa, “Análise de Artefactos em Campanhas de Phishing,” *Revista de Cibersegurança e Privacidade*, vol. 7, no. 1, pp. 15–27, 2023.
[3] A. Flores and T. Bennett, “Dynamic Analysis of Malicious Telegram Channels,” *Proceedings of the International Conference on Cyber Threat Intelligence*, pp. 112–120, 2022.
[4] European Cybersecurity Organization, “Annual Cyber Threat Report: Trends and Challenges,” 2023. [Online]. Available: https://www.eu-cybersec.org
[5] T. Holz et al., “Measuring and Detecting Malicious Telegram Channels,” *NDSS Symposium*, 2024.
[6] Symantec, “Global Trends in Cybersecurity Threats,” Symantec Threat Report, 2023. [Online]. Available: https://www.symantec.com
[7] R. Vasconcelos, “Infraestruturas de Comando e Controle: Análise e Monitorização em Operações de Phishing,” *Conferência Internacional de Segurança Cibernética*, pp. 85–94, 2023.
[8] J. Anderson and R. Smith, “Exploring Telegram's Role in Modern Phishing Campaigns,” *Cybercrime Research Quarterly*, vol. 9, no. 2, pp. 34–49, 2022.
[9] A. Wichmann et al., “Covert Access to Encrypted Messaging Services for Cyber Threat Intelligence,” *ACM CCS*, 2023.
[10] MITRE ATT&CK, “Tactics, Techniques and Procedures: Messaging Platforms,” 2024. [Online]. Available: https://attack.mitre.org
[11] Kaspersky Lab, “Telegram Threat Landscape: 2023 Report,” 2023. [Online]. Available: https://www.kaspersky.com/telegram-threats-report

[12] J. Alves, A. Respício, I. Rosa and P. Rodrigues, "Threat Intelligence - Improving SIEM cybercriminality awareness using information from IP blacklists," *eCrime2017.EU - APWG.EU Symposium on Electronic Crime Research*, Porto, Portugal, 2017.
[13] J. Alves, "Threat Intelligence: Using OSINT and Security Metrics to Enhance SIEM Capabilities," M.Sc. Thesis, Faculdade de Ciências, Universidade de Lisboa, 2017.
[14] S. Kumar, B. Janet, and R. Eswari, "Multi Platform Honeypot for Generation of Cyber Threat Intelligence," *2019 IEEE 9th International Conference on Advanced Computing (IACC)*, 2019.
[15] M. Bromiley, "Threat Intelligence: What It Is, and How to Use It Effectively," SANS Institute Reading Room, 2016.
[16] I. Rosa et al., "Cyber Threat Intelligence Architecture for Applied Cybersecurity Scenarios," *17th Iberian Conference on Information Systems and Technologies (CISTI)*, Madrid, 2022.
[17] D. Fidler, "Ethical and Legal Dilemmas in Covert Cyber Surveillance," Ethics & Information Technology, vol. 24, no. 1, pp. 77–92, 2022.
[18] G. Disterer, Cyber Threat Intelligence: Data Sharing, Automation, and Risk Assessment. Springer, 2024. DOI: 10.1007/978-3-031-54497-2
[19] R. Wörner and S. Haas, "Natural Language Processing for Threat Detection: Emerging Trends and Case Studies," *AI & Cybersecurity Journal*, vol. 5, no. 2, pp. 60–78, 2024. DOI: 10.1007/s43681-024-00427-4