https://doi.org/10.58086/hbgd-e714

MALVERTISING AS A VECTOR OF CYBERCRIME IN DIGITAL PLATFORMS

João Sousa[1]✉, **Mário Dias Lousã**[1,2], **José Carlos Morais**[1,3]

[1] Instituto Superior Politécnico Gaya (ISPGAYA), Portugal.
[2] Insight - Piaget Research Center for Ecological Human Developement, Portugal.
[3] CEOS.PP, ISCAP, Polytechnic of Porto, Portugal..
✉ Corresponding authors**:** ispg2024104121@ispgaya.pt

Abstract

The usage of malvertising, which exploits advertising networks to send malware, ransomware, and phishing techniques while evading traditional security measures, has become a significant avenue for criminality on digital platforms. This study provides a bibliometric analysis of 236 papers from The Lens database, focusing on the evolution of scientific output, author collaboration patterns, and theme frameworks in malvertising research. Using Bibliometrix (R) and VOSviewer, co-authorship networks, keyword co-occurrence maps, theme clusters, and a density metadata table were created to identify research trends and knowledge gaps. Results show that machine learning, behavioral analytics, and ecosystem-aware security solutions are receiving more attention in the field of research, with high-impact publications like IEEE Access, Sensors, and Electronics making substantial contributions to their development. Additionally, the report highlights research prospects and difficulties by identifying upcoming issues such as blockchain, IoT, AR/VR platforms, and zero-day malvertising. Finally, this report summarizes the state of the art in malvertising research, highlights systemic weaknesses in advertising ecosystems, and offers suggestions for future cybersecurity research topics, adaptive defense tactics, and regulation.

Keywords: Malvertising, Online Advertising Ecosystems, Cybercrime, Malware Distribution, Bibliometric Analysis.

1. Introduction

Digital advertising has become a dominant method of distributing publicity over the past two decades, attracting substantial revenue and integrating deeply into online ecosystems (Sadeghpour & Vlajic, 2021). Due to its growth and scale, it has also become a target for

cybercriminals, who exploit ad networks to deliver malicious content and compromise users (Nowroozi et al., 2022). Malvertising has emerged as a key vector for cybercrime campaigns, where attackers embed ads and exploit kits to bypass traditional security controls (Anand et al., 2023). With the development of mobile applications, the progression of technology further extends the threat, as some apps deliver malicious ads or redirect users to harmful content (Liu et al., 2020). On social media platforms, attackers disguise themselves as legitimate advertisers to target users with harmful ads, leveraging micro-targeting to maximize exposure (Arrate et al., 2020). Despite the rapid growth of research on digital advertising threats, current literature presents malvertising as a vector for cybercrimes (Pooranian et al., 2021). Studies highlight vulnerabilities across the entire advertising ecosystem, including publishers, exchanges, and DSP/SSP networks, yet systematic analyses of prevalence, mechanics, and technological enablers remain scarce (Chua et al., 2020). Recent reviews highlight that malvertising is an initial access technique and is able to partake in complex exploit-kit supply chains, but comprehensive mappings of trends, thematic structures, and author networks are still lacking (Caviglione et al., 2021). This gap defines the need for a bibliometric approach to identify research clusters, emerging topics, and patterns of collaboration in malvertising studies.

A bibliometric analysis was chosen for this study, as it favors an approach where the author examines the scientific research done about malvertising. By analyzing publication patterns, author collaborations, and keyword trends, this method allows for a clear mapping of research activity and thematic development in the field. To ensure the transparency and reproducibility of the process for selecting and screening relevant studies through the recurrent application of the PRISMA 2020 framework. With the usage of bibliometric techniques, it's expected that it will be possible to extract results about the current state of research while highlighting general trends and structures without overextending the available data. The main objective of this study is to analyze the scientific literature on malvertising as a vector of cybercrime in digital platforms using bibliometric techniques, with a particular focus on publication trends, thematic structures, and the evolution of research over time. To achieve this goal, the study addresses the following research questions:

RQ1: How has the scientific production on malvertising evolved over time?

RQ2: What author clusters and collaboration patterns can be identified in malvertising research?

RQ3: What are the main keyword clusters and conceptual structures shaping malvertising research?

RQ4: What are the dominant research themes and topics addressed in the literature on malvertising?

RQ5: How is the scientific literature on malvertising distributed in terms of research density and thematic concentration?

This paper is composed of six sections as follows. In section one, there is an introduction to the study, contextualizing malvertising as a critical vector of cybercrime in digital platforms. Section two provides a theoretical conceptualization of malvertising, outlining its main definitions, mechanisms, and relationship with cybercrime and the way cybercriminals act. The bibliometric methodology used is presented in section three, including data sources, search strategy, and analytical techniques. Section four presents the results of the bibliometric analysis, including author and keyword clusters, publication trends, and density maps. Following the results retrieved from section four, we have section five, where the discussion of the main findings and their implications for research and practice is done. Finally, section six concludes the paper by summarizing the results, highlighting limitations, and suggesting directions for future research.

2. Theoretical Conceptualization

2.1. Malvertising

In cybercrime, there are several ways to attack users, such as malvertising, where malicious code is injected into legitimate advertising content, or a connection is introduced that takes the user to a third-party website, enabling attackers to deliver malware without the user's knowledge (Pooranian et al., 2021). It is particularly effective because it operates within environments that users already view as trustworthy. The attackers responsible for these types of crimes often navigate into popular websites, creating automated connections between users and malware distribution sites, a tactic frequently leveraged in malvertising campaigns (Shin et al., 2022). Unlike traditional attack vectors that rely on explicit user interaction, malicious advertisements are delivered through browsing activities, reducing user suspicion and increasing exposure to attacks. This type of attack typically employs

obfuscated scripts and invisible iframes to redirect users to exploit kits or malware-hosting domains, evading conventional detection systems (Shin et al., 2022). Such operations follow a standard pipeline in which an advertisement leads to a redirect chain, which then directs the user to an exploit kit that delivers a tailored payload, allowing attackers to customize malware delivery based on the user distraction or not having knowledge about the danger without requiring user consent (Caviglione et al., 2021). Such characteristics make this type of cybercrime difficult to detect and mitigate, as the contents are often indistinguishable from legitimate advertising until the attack and proceeding exploitation occur.

2.2. Digital Advertising Ecosystem

The modern online advertising ecosystem is composed of multiple intermediaries, including ad networks, ad exchanges, supply-side platforms, demand-side platforms, and data management platforms, which connect publishers, advertisers, and users (Sadeghpour & Vlajic, 2021). With the fact that digital advertising is highly automated by nature, there are further complications in the case of security enforcement, as decisions related to ad placement and delivery are often executed in milliseconds with minimal human oversight. While these intermediaries enable efficient targeting and monetization, they also expand the attack surface for fraud and malvertising (Sadeghpour & Vlajic, 2021). Also, there are limits to the ability to conduct thorough security validation at each stage of the advertising process due to the speed and efficiency of security checks and the revenue generation priority. This increases the dangers for ad viewers. With the rise in the topic of fraud, there was a necessity to create categories such as placement fraud, traffic fraud, and action fraud, with malvertising being categorized as a key form of placement fraud (Sadeghpour & Vlajic, 2021). Lack of transparency in ad brokerage processes and the speed of real-time bidding systems further complicate creative vetting, allowing malicious ads to bypass security checks (Caviglione et al., 2021). As a result of the current framework, security responsibilities are frequently distributed across multiple employees of the ad platforms, creating gaps that can be exploited by malicious actors.

2.3. Cybercrime Campaigns via Malvertising

With the rise of cybercrime operations, the malvertising in the multiple vectors the cybercriminals use to attack and steal from the multiple digital platform users is done with such strategic thinking. Nowadays most of the used attack vectors are shifting toward low-interaction, high-reach attack models. Malvertising is increasingly being used in broader cybercrime campaigns, including ransomware, phishing, and crypto mining operations (Anand et al., 2023). To achieve a large-scale malware distribution with low maintenance, the cybercriminals use the fact that the advertising channels don't have high levels of security and ad checks in a way to create direct engagement with victims. Attackers exploit advertising infrastructure to deliver malware payloads while bypassing traditional security controls, using malicious ads as covert delivery channels (Nowroozi et al., 2022). Also, the development of mobile applications further extends this threat, delivering harmful ads or redirecting users to malicious content (Liu et al., 2020). Social media platforms amplify the risk, as attackers masquerade as legitimate advertisers or deploy automated bots to distribute fake advertisements and manipulate engagement metrics (Mbona & Eloff, 2021). This framework that the platforms use not only increases campaign efficiency but also complicates attribution and disruption efforts, as malicious activity is embedded within legitimate commercial infrastructures. Malvertising campaigns also exploit weaknesses in digital platforms using plugins, leveraging user trust and executing plugins to take over the privileges of those who fall and are infected to trigger ad injections or redirects across multiple pages (Kasturi et al., 2022).

2.4. Security Implications and Detection Challenges

The usage of malicious advertisement URLs has become challenging to detect because they often mimic legitimate sites and evolve rapidly, rendering traditional detection methods ineffective (Nowroozi et al., 2022). One of the primary difficulties in addressing malvertising lies in the transient nature of malicious advertising content, which frequently remains active only for short periods, rotating domains, scripts, and delivery mechanisms to avoid sustained exposure. The fact that this behavior is short-lived reduces the effectiveness of retrospective analysis and limits the usefulness of static threat intelligence, requiring detection systems to

operate under strict time constraints. To combat this type of cybercrime, certain detection strategies include rule-based approaches, which rely on predefined indicators, and behavioral analysis using machine learning to classify URLs based on patterns and features. Lexical and web-scraped features, such as URL length, domain age, WHOIS information, and HTML structure, improve classification accuracy when combined (Nowroozi et al., 2022). Another challenge arises from the differences between detection accuracy and operational scalability, which make it so that the digital platforms that are already processing vast volumes of advertisements and user interactions in real time leave limited computational resources for deep inspection or complex behavioral analysis. As a result, security mechanisms must balance precision with performance, often prioritizing lightweight detection methods that may be less effective against sophisticated or well-obfuscated malvertising campaigns. Malvertising campaigns base the mode of operation on the exploitation of social trust and branding cues to increase perceived legitimacy, particularly through counterfeit or fake advertisements and popular styles of posts that mimic sponsorships (Grigsby, 2020). Additionally, rehosting vulnerabilities allow attackers to bypass protections, inject scripts, and persist in client-side attacks, reflecting the socio-technical complexity of malvertising as both a lure and a payload delivery mechanism (Watanabe et al., 2020). The involvement of multiple intermediaries and third-party services obscures the origin of malicious content, making it difficult to trace attacks back to their source, making it challenging to attribute faults and respond to incidents. Finally, getting to the main problem is that the lack of transparency and accountability makes clear that the takedown efforts and delays in responses are allowing campaigns to persist across different platforms and regions. One way to reduce the attacks of malvertising exploits is to install ad and tracking blockers to mitigate exposure by preventing ad and tracker requests (Borgolte & Feamster, 2020). Tackling these challenges together demonstrates that malvertising detection cannot rely solely on isolated technical indicators or user-side protections. Instead, effective defense requires adaptive mechanisms that account for the dynamic behavior of advertising content, the scale of modern ad delivery systems, and the human factors that influence user interaction. Addressing these dimensions collectively is essential for improving resilience against evolving malvertising threats.

3. Methodology

The study structure selected for this scientific literature on malvertising as a vector of cybercrime in digital platforms was the bibliometric approach. Data was retrieved from The Lens database, selected for its extensive coverage, detailed metadata exports, and compatibility with bibliometric tools.

The PRISMA 2020 framework (Figure 1) guided the selection process, providing a structured approach to ensure transparency and rigor in paper screening. With the initial search returning 442 records. Filters for document type (journal article), presence of abstract and full-text, and English language, along with duplicate removal, were applied, resulting in a final dataset of 236 papers.

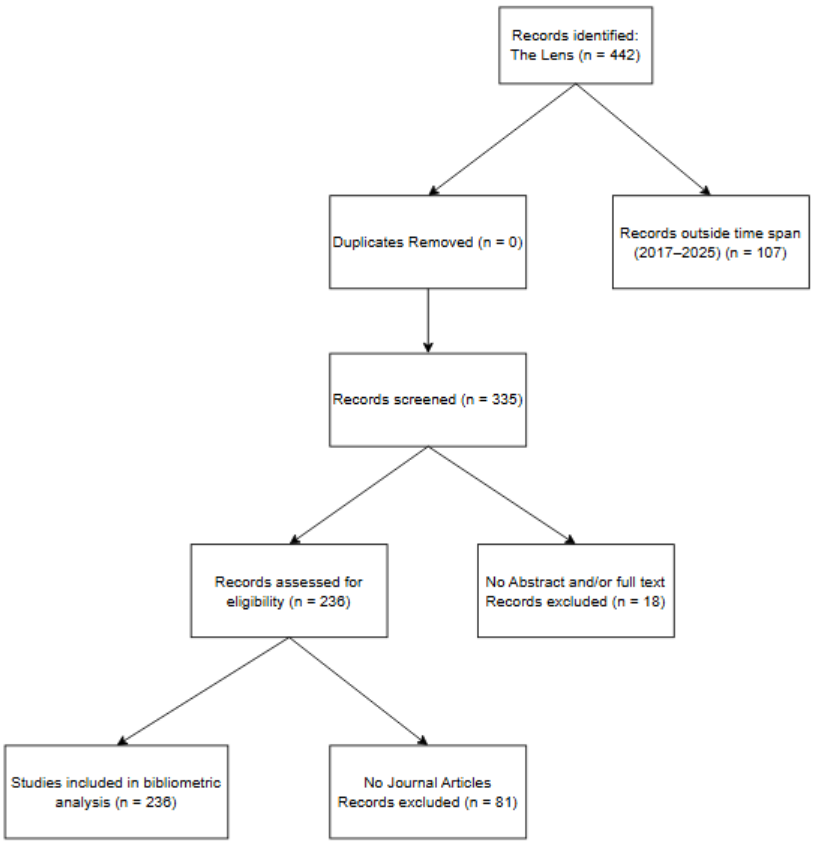

Fig 1. PRISMA flow diagram
Source: Authors' elaboration.

The search query was created to capture the scientific literature related to malicious advertising as a cybersecurity threat. Recurring to the usage of a combination of multiple terms related to malvertising, including malicious advertising, ad-based malware, ad fraud, drive-by downloads, exploit kits, and malware distribution through online advertisements,

ensuring broad coverage of attack techniques and delivery mechanisms. Then these terms are restricted by cybersecurity-related concepts, such as cybersecurity, information security, web security, browser exploits, malware delivery, and threat vectors, to focus the results on security-oriented studies. The query also includes platform-level and ecosystem-specific terms, in particular advertising platforms, ad networks, ad exchanges, adtech, and real-time bidding (RTB), enabling the identification of research addressing the technical and infra-structural dimensions of malvertising within digital advertising environments. With this structured combination, the aim is to have both thematic relevance and comprehensive cov-erage of the domain.

In the metadata extracted, it included authors, publication years, keywords, affiliations, and sources. The analyses were conducted using VOSviewer and Bibliometrix (RStudio) to gen-erate co-authorship networks, identify clusters of collaborating researchers, and map key-word co-occurrence to detect prevalent themes and subtopics. Density and topic maps were used to visualize thematic clusters, and annual publication illustrated the evolution of re-search activity and influence over time. Additional metrics taken included the identification of the most relevant sources, providing an overview of collaboration patterns and thematic structures in malvertising research.

Metadata	Description	Missing Counts	Missing %	Status
DI	DOI	0	0.00	Excellent
DT	Document Type	0	0.00	Excellent
SO	Journal	0	0.00	Excellent
PY	Publication Year	0	0.00	Excellent
TI	Title	0	0.00	Excellent
TC	Total Citation	0	0.00	Excellent
AB	Abstract	2	0.85	Good
AU	Author	2	0.85	Good
DE	Keywords	43	18.22	Acceptable
ID	Keywords Plus	43	18.22	Acceptable
CR	Cited References	54	22.88	Poor
C1	Affiliation	236	100.00	Completely missing
RP	Corresponding Author	236	100.00	Completely missing
LA	Language	236	100.00	Completely missing
WC	Science Categories	236	100.00	Completely missing

Fig 2. Density visualization of the metadata
Source: Bibliometrix output (2025).

4. Results

This segment offers a detailed descriptive overview of the bibliometric outcomes, establishing the basis for the following discussion and examination of the results. The findings are illustrated through network maps, tables, and visual analyses, providing an overview of the scientific research done about the selected literature. The results are organized to highlight key structural components of the research domain, such as publication trends, author collaboration networks, and the most prevalent themes and concepts. Each figure and table is examined individually, ensuring a clear and structured comprehension of the identified trends.

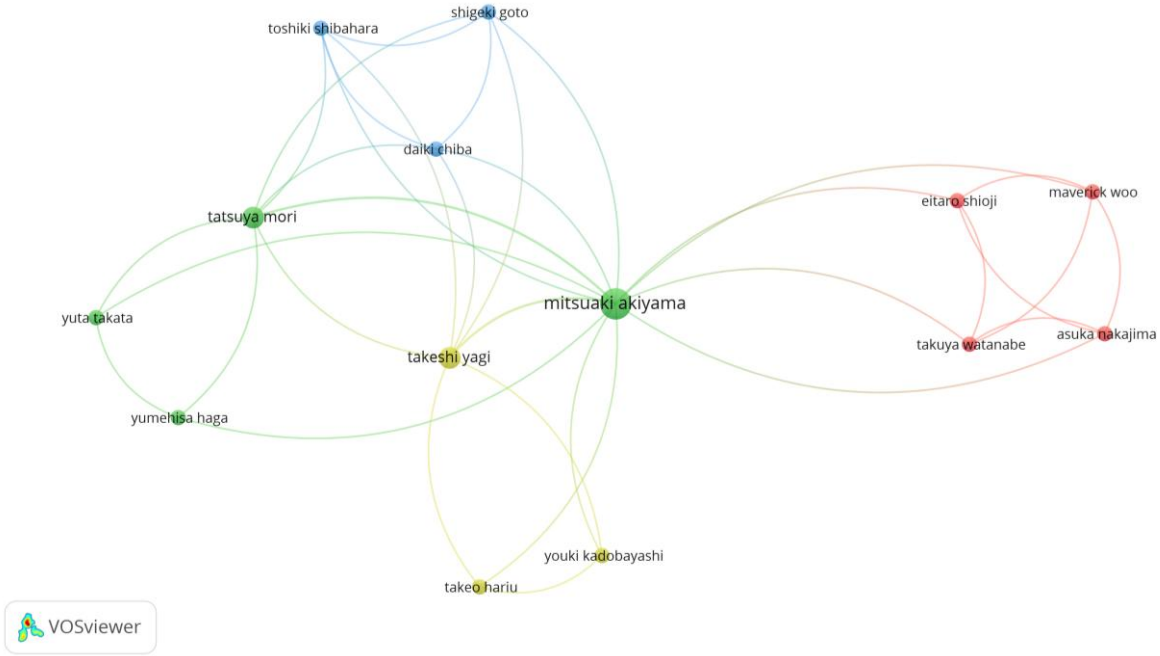

Fig 3. Co-authorship network of authors
Source: VOSviewer outputs (2025).

The co-authorship network (Figure 3) displays a map of the information collected from The Lens database and created with VOSviewer, highlighting the collaborative framework of scientific inquiry into malvertising as a means of cybercrime on digital platforms. The network comprises authors who have published at least one document and possess no fewer than two co-authorship links, guaranteeing that the map reflects recognized collaboration patterns instead of individual contributions. Authors are categorized into unique clusters, with each cluster representing research teams or collaborative groups created through co-authorship of publications.

It also illustrates various clusters that depict a fragmented but organized research environment. Writers with greater total link strength and citation totals hold more central roles in their clusters, signifying a stronger collaborative influence and greater scientific impact. Also, the smaller clusters are made up of authors who have fewer works and lower citation metrics, indicating more niche or developing research areas. The physical distance among clusters signifies restricted collaboration between groups, representing chances for wider cooperation among research communities to enhance and unify knowledge generation in the realms of malvertising and cybersecurity.

The network illustrated in Figure 4 represents the co-occurrence of author-defined keywords, considering a minimum occurrence threshold of five documents. This visualization captures the underlying conceptual organization of the literature on malvertising and cybersecurity, revealing how frequently used terms are interconnected across the analyzed studies. Central nodes such as “cybersecurity”, “cyber security”, and “cybercrime” occupy important positions in the network, reflecting their transversal role across the analyzed publications. These terms show strong connections with keywords related to malicious activities and threat vectors, including “malware”, “ransomware”, “phishing”, and “cyber attacks”, indicating a research focus on the use of online platforms and advertising infrastructures as key objectives for cybercrime.

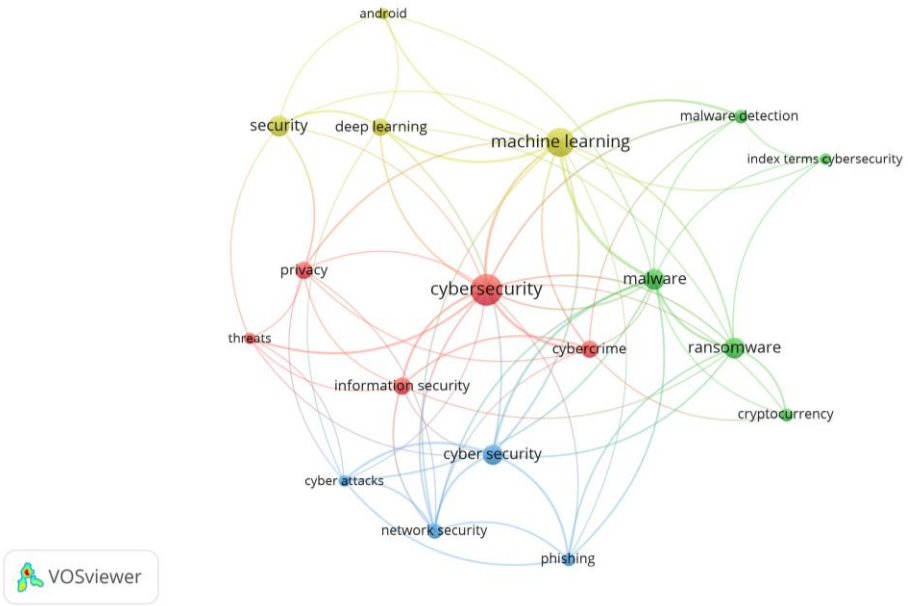

Fig 4. Keyword co-occurrence network
Source: VOSviewer outputs (2025).

Distinct thematic clusters can be observed. One cluster emphasizes technical detection and mitigation approaches, bringing together terms such as “machine learning”, “deep learning”, and “malware detection”, which suggests a growing reliance on data-driven techniques to identify malicious advertising campaigns. Another cluster is associated with platform and ecosystem contexts, including keywords such as “android”, “network security”, and “privacy”, highlighting concerns related to mobile environments and user protection. Overall, the keyword co-occurrence network illustrates a field structured around the intersection of cybersecurity, malware distribution mechanisms, and advanced analytical techniques, with increasing attention to automated detection and platform-specific threats.

Figure 5 represents the co-occurrence network of frequently used terms taken from the reviewed papers, focusing solely on terms referenced at least ten times and appearing in multiple articles. This map emphasizes frequently employed concepts in literature, providing a comprehensive summary of the prevalent terminology and recurring research topics in investigations related to malvertising and cybersecurity.

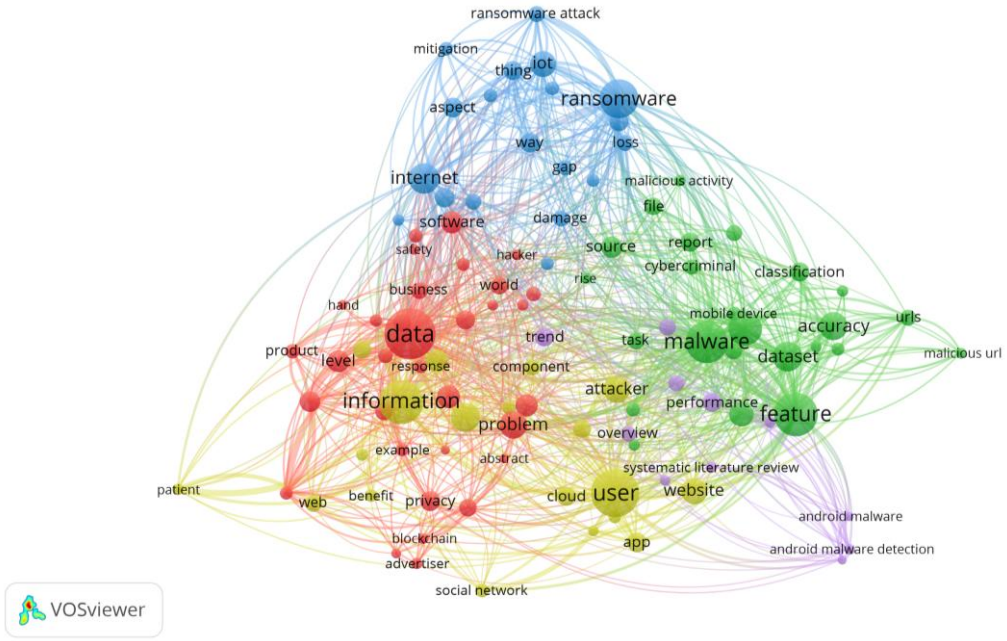

Fig 5. Common-term co-occurrence network in malvertising and cybersecurity literature
Source: VOSviewer outputs (2025).

The network shows multiple dense clusters that indicate unique yet interrelated research domains. A significant grouping highlights ideas related to data and detection, including terms like data, algorithm, feature, dataset, machine learning, and malware detection, reflecting a strong focus on analytical and computational methods. A different cluster organizes terms associated with threats and attack dynamics, including attacker, cybercrime,

ransomware, botnet, phishing, and malicious activities, emphasizing the operational viewpoint of cybercrime activities. The topics mobile and platforms arise from recurring terms such as android, mobile device, app, online advertising, and websites, highlighting the significance of digital platforms as avenues for harmful actions. The occurrence and concentration of terms indicate that the literature merges particular detection techniques with wider discussions regarding cyber threats, user impacts, and platform vulnerabilities, underscoring the interdisciplinary aspect of malvertising studies.

The evolution of scientific output from 2017 until 2025 shows significant annual variations in publication counts (Figure 6). From 2017 to 2019, the total of publications rose from 21 to 32, reflecting an increasing focus on research in this area. Scientific output reached its highest point in 2020 with 48 publications, then experienced a minor drop to 40 in 2021, before a small increase to 44 in 2022. Following 2022, a significant decline is observed, leading to 21 publications in 2023 and only seven in each of 2024 and 2025, mainly due to constraints in data gathering for the recent years. This trend illustrates the dynamic nature of research in malvertising and cybersecurity, highlighting periods of intensified academic attention as well as the current stabilization phase.

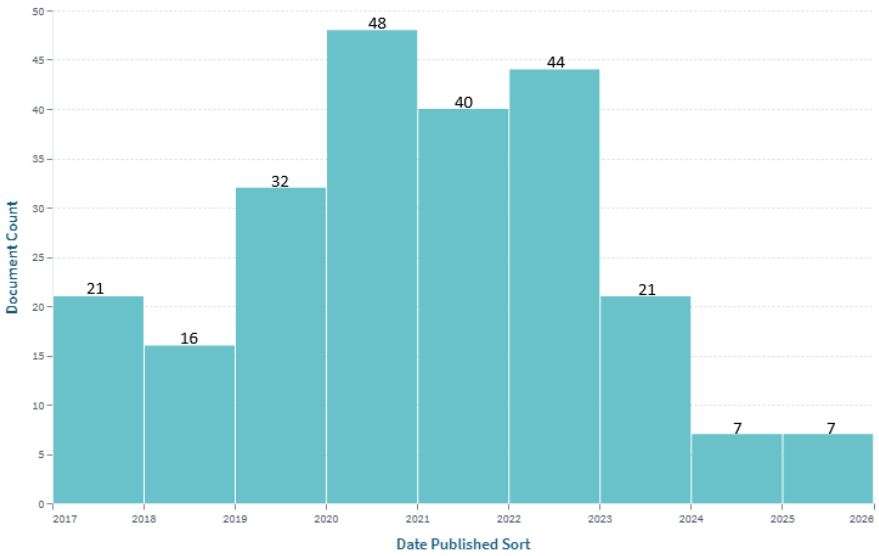

Fig 6. Annual scientific production on malvertising-related cybersecurity research
Source: The Lens database (2025).

The thematic map consists of four primary quadrants (Figure 7): Motor Themes, Basic Themes, Niche Themes, and Emerging or Declining Themes, arranged according to two axes: development degree represented on the vertical axis and relevance degree included on the horizontal axis. Fields such as machine learning, cybersecurity, and deep learning are

well developed and prominent in the upper-right quadrant with the Motor Themes, signifying established domains with strategic significance for upcoming research. In the lower-right quadrant are included the Basic Themes with malware, ransomware, cryptocurrency, cybersecurity, and information security, which constitute the foundation of the field. While not as focused as motor themes, these topics show considerable importance but lower density, providing a conceptual and practical foundation for study.

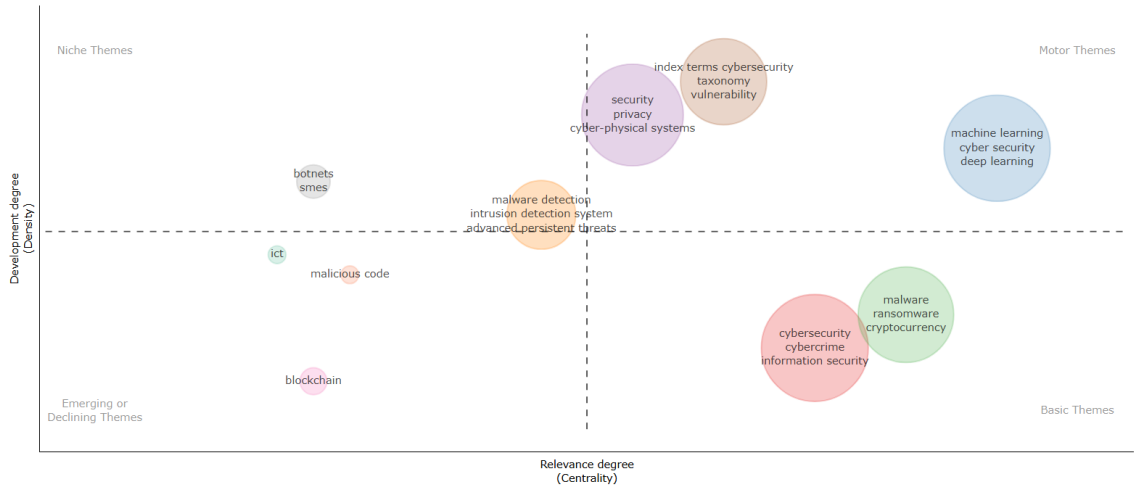

Fig 7. Thematic map of research topics on malvertising and cybersecurity
Source: Bibliometrix (2025).

The upper-left quadrant represents the Niche Themes with subjects such as security privacy, cyber-physical systems, and vulnerability taxonomy. These subjects show high density but low centrality, suggesting extensive research in specific subfields that have minimal broader influence. The lower-left quadrant appears the Emerging or Declining Themes which feature Blockchain, ICT, and malicious code, characterized by low density and low centrality, signifying either initial development or possible decline. In conclusion, this map illustrates that the incorporation of artificial intelligence in cybersecurity, particularly via machine learning and deep learning, is presently guiding research initiatives, while malware and ransomware remain crucial topics. With the continuous advancement of technology and cyber threats, emerging fields like blockchain and malicious software may gain greater importance.

Table 1 shows the most relevant sources in scientific production in malvertising and cybersecurity. The data indicate that a sizable portion of the papers is concentrated in leading sources, such as IEEE Access (17 articles), Sensors (Basel, Switzerland) (13 papers), and

Electronics (12 papers). Other important sources include Applied Sciences (8 papers), SSRN Electronic Journal (6 papers), Security and Communication Networks (5 papers), Information (4 papers), International Journal of Advanced Computer Science and Applications (4 papers), International Journal of Information Security (4 papers), and Journal of Cyber Security and Mobility (4 papers). These results highlight the sources that contribute most to the field, reflecting the thematic spread across cybersecurity, computer science, and electronic engineering. Also, let's not forget that even if these sources do fit in with the top publication sources, they only compose 77 papers out of the 236 analyzed. This means that smaller sources also impacted the field with research, with 159 papers published, but some with only 2/3 maximum per source.

Table 1. Top 10 publication sources in malvertising and cybersecurity research

Source	Articles
IEEE Access	17
Sensors (Basel, Switzerland)	13
Electronics	12
Applied Sciences	8
SSRN Electronic Journal	6
Security and Communication Networks	5
Information	4
International Journal of Advanced Computer Science and Applications	4
International Journal of Information Security	4
Journal of Cyber Security and Mobility	4

Source: Authors' elaboration based on data from The Lens database (2025).

5. Discussion

5.1. Patterns and Trends

The bibliometric review reveals that conventional blacklist approaches for detection are inadequate to manage the changing and evolving characteristics of harmful URLs, stressing the need for adaptive and smart detection methods. The significance of regularly refreshing detection models and refining feature selection is highlighted, guaranteeing that new attack patterns can be successfully addressed within digital advertising networks (Shin et al., 2022). Exploit kits paired with malvertising demonstrate the weaponization of advertising

ecosystems, facilitating widespread infection by diverting users from legitimate ad spaces to compromised landing pages (Usharani et al., 2021).

5.2. Analysis of Key Authors, Institutions, and Sources

The leading sources and authors indicate a focus of research activities in influential publications and niche investigations. Although bibliometric data does not enable a direct analysis at the country's level, the significance of institutions like IEEE Access, Sensors, and Electronics (leading sources) suggests a concentration of academic activity in technologically advanced research centers. The networks of co-authorship and patterns of institutional production indicate a cooperative atmosphere, frequently among authors who emphasize detection methods and analyses at the ecosystem level. These results, aligned with earlier studies, highlight the importance of centralized research teams in enhancing understanding of malvertising and cybersecurity.

Comparison with Previous Studies

Previous studies show that malicious ads often give themselves away through long URLs, fake domains, or direct IP addresses. However, the GandCrab project proved that malvertising has evolved into much more than simple ad fraud. It is now a primary way to spread ransomware, which creates an urgent need for better security in ad networks and more advanced tools to catch exploit kits (Nowroozi et al., 2022). At the same time, bot-driven spam remains a major risk because these automated systems are now excellent at mimicking real human behavior (Mbona & Eloff, 2021). More recently, research has found that malvertising is becoming a standard part of the Ransomware-as-a-Service model. This trend exploits the vulnerabilities found in automated bidding and the industry's heavy reliance on third parties (Anand et al., 2023). Overall, these findings show that we should no longer view malvertising as a series of isolated tricks but rather as a systemic threat to the entire digital ecosystem.

Thematic Analysis and Evolution of Topics

The thematic clusters identified in the keyword analysis reveal an evolution from intrusion detection-focused research to approaches emphasizing machine learning, behavioral analytics, and ecosystem resilience. Malvertising's systemic impact includes user compromise, erosion of ecosystem trust, and financial losses, often compounded by click fraud to

maximize revenue. The discussion of countermeasures includes consistent validation of ad content, the implementation of anti-malware tools, and detection techniques based on machine learning, like SVM classifiers trained on features of suspicious ads. Nonetheless, current models are usually confined to recognized attack patterns, rendering systems susceptible to zero-day malvertising risks. Newly developed solutions, such as game-theoretic defenses, dynamic traffic analysis, and blockchain-driven transparency, offer ways to strengthen ad-tech security principles and address the multifaceted, programmatic, and RTB-enhanced dangers brought by malvertising (Pooranian et al., 2021). Significantly, sophisticated methods like PhishTransformer utilize CNN and Transformer encoders to examine URLs in ad frames and scripts, attaining cutting-edge precision, recall, and F1-scores while simplifying detection complexity (Asiri et al., 2024). Moreover, machine learning and data-driven methods, such as publisher-side SVM classifiers and MadTracer rules, facilitate extensive malvertising detection, although they depend significantly on current heuristics and strong feature engineering. The literature further anticipates that emerging platforms such as IoT and AR/VR will become future malvertising targets, highlighting the need to apply current defense mechanisms, such as sandboxing, behavioral analysis, and secure ad SDKs, to these new digital endpoints (Chua et al., 2020).

6. Conclusion

This bibliometric analysis offers an extensive overview of malvertising research, highlighting trends in publication, author partnerships, and thematic development. The findings underscore the shortcomings of conventional detection methods, like blacklists, and stress the rising use of adaptive, machine learning-driven strategies to combat advancing cyber threats. The co-authorship networks indicate possibilities for wider interdisciplinary cooperation, whereas leading sources and recognized research groups prevail in the domain. This research focuses on The Lens database and English-language publications, revealing prominent research domains such as malware detection, ecosystem vulnerabilities, and AI-based defense methods. In addition, new topics like blockchain incorporation, IoT and AR/VR security, and zero-day malvertising, presenting possibilities for future research.

In conclusion, the information available shows that malvertising serves not just as a means of ad fraud but also as a pervasive cybercrime risking users, platforms, and advertising

networks. The findings offer important perspectives for both researchers and users, informing the creation of stronger detection systems, real-time surveillance frameworks, and forward-thinking cybersecurity strategies. With the evolution of malvertising, the future of research will be based on adaptive defense mechanisms, evolving digital platforms, and cross-disciplinary methods required to address the increasing issues caused by malvertising, using integrated temporal, collaborative, and thematic aspects of research.

References

Anand, P. M., Charan, P. V. S., & Shukla, S. K. (2023). HiPeR – Early detection of a ransomware attack using hardware performance counters. *Digital Threats: Research and Practice, 4*(3), Article 43, 1–24. https://doi.org/10.1145/3608484

Arrate, A., González-Cabañas, J., Cuevas, Á., & Cuevas, R. (2020). Malvertising in Facebook: Analysis, quantification and solution. *Electronics, 9*(8), 1332. https://doi.org/10.3390/electronics9081332

Asiri, S., Xiao, Y., & Li, T. (2024). PhishTransformer: A novel approach to detect phishing attacks using URL collection and transformer. *Electronics, 13*(1), 30. https://doi.org/10.3390/electronics13010030

Borgolte, K., & Feamster, N. (2020). Understanding the performance costs and benefits of privacy-focused browser extensions. In *Proceedings of The Web Conference 2020* (pp. 2275–2286). ACM. https://doi.org/10.1145/3366423.3380292

Chua, M. Y.-K., Yee, G. O. M., Gu, Y. X., & Lung, C.-H. (2020). Threats to online advertising and countermeasures: A technical survey. *Digital Threats: Research and Practice, 1*(2), Article 11, 1–27. https://doi.org/10.1145/3374136

Caviglione, L., Choras, M., Corona, I., Janicki, A., Mazurczyk, W., Pawlicki, M., & Wasielewska, K. (2021). Tight arms race: Overview of current malware threats and trends in their detection. *IEEE Access: Practical Innovations, Open Solutions*, *9*, 5371–5396. https://doi.org/10.1109/access.2020.3048319

Grigsby, J. L. (2020). Fake ads: The influence of counterfeit native ads on brands and consumers. *Journal of Promotion Management*, *26*(4), 569–592. https://doi.org/10.1080/10496491.2020.1719958

Kasturi, R. P., Fuller, J., Sun, Y., Chabklo, O., Rodriguez, A., Park, J., & Saltaformaggio, B. (2022). Mistrust plugins you must: A large-scale study of malicious plugins in WordPress marketplaces. In *Proceedings of the 31st USENIX Security Symposium* (pp. 161–178). USENIX Association.

Liu, T., Wang, H., Li, L., Luo, X., Dong, F., Guo, Y., Wang, L., Bissyandé, T. F., & Klein, J. (2020). MadDroid: Characterizing and detecting devious ad contents for Android apps. In

Proceedings of The Web Conference 2020 (pp. 1715–1726). ACM. https://doi.org/10.1145/3366423.3380242

Mbona, I., & Eloff, J. H. P. (2022). Feature selection using Benford's law to support detection of malicious social media bots. *Information Sciences, 582,* 369–381. https://doi.org/10.1016/j.ins.2021.09.038

Nowroozi, E., Abhishek, Mohammadi, M. R., & Conti, M. (2022). An adversarial attack analysis on malicious advertisement URL detection framework. *IEEE Transactions on Network and Service Management.* Advance online publication. https://doi.org/10.48550/arXiv.2204.13172

Pooranian, Z., Conti, M., Haddadi, H., & Tafazolli, R. (2021). Online advertising security: Issues, taxonomy, and future directions. *IEEE Communications Surveys & Tutorials, 23*(4), 2494–2524. https://doi.org/10.1109/COMST.2021.3118271

Sadeghpour, S., & Vlajic, N. (2021). Ads and fraud: A comprehensive survey of fraud in online advertising. *Journal of Cybersecurity and Privacy, 1*(4), 804–832. https://doi.org/10.3390/jcp1040039

Shin, S.-S., Ji, S.-G., & Hong, S.-S. (2022). A heterogeneous machine learning ensemble framework for malicious webpage detection. *Applied Sciences, 12*(23), 12070. https://doi.org/10.3390/app122312070

Usharani, S., Manju Bala, P., & Martina Jose Mary, M. (2021). Dynamic analysis on crypto-ransomware by using machine learning: GandCrab ransomware. *Journal of Physics: Conference Series, 1717,* 012024. https://doi.org/10.1088/1742-6596/1717/1/012024

Watanabe, T., Shioji, E., Akiyama, M., & Mori, T. (2020). Melting pot of origins: Compromising the intermediary web services that rehost websites. *Proceedings of the Network and Distributed Systems Security (NDSS) Symposium 2020* (pp. 1–15). Internet Society. https://doi.org/10.14722/ndss.2020.24140