Identifying Illicit Online Health Marketplaces

Team #4

Taiga Asanuma
tasanuma@ucla.edu
Ying Li
ying.li@ucla.edu
Yufei Song
yufeisong@ucla.edu
Zihan Wang
zihan0312@ucla.edu

May 30, 2025

Identifying Illicit Online Health Marketplaces

Taiga Asanuma
University of California, Los Angeles

Ying Li
University of California, Los Angeles

Yufei Song
University of California, Los Angeles

Zihan Wang
University of California, Los Angeles

Abstract

In this paper, we analyze the effectiveness of utilizing large language models (LLMs) to detect Illicit Online Pharmacies (IOPs). Specifically, we examine keyword strategies for filtering Censys scan data, the common hosting characteristics of IOPs, the accuracy of newly identified IOPs through LLMs, and how LLMs can augment traditional manual detection methods. The results demonstrate that LLMs are effective in identifying IOPs that human-only keyword lists would not detect, as well as in automating the time-consuming task of classifying websites as illicit or legitimate. LLMs identified 245 confirmed illicit online pharmacies (IOPs) from over 6,400 previously undetected hosts. Although LLMs demonstrated lower precision than manual methods, combining the two approaches offers strong potential for a hybrid detection framework that leverages their complementary strengths. In light of the limited protection offered by existing blocklists, this work aims to serve as a starting point for developing an LLM-enhanced blocklist better equipped to detect and protect users from IOPs.

1 Introduction

Illicit online health marketplaces have emerged as a critical threat to global public health. These platforms often promote and sell unauthorized pharmaceutical products, counterfeit medications, and controlled substances without valid prescriptions. [8] The accessibility and anonymity provided by the Internet have enabled such actors to operate with growing sophistication, bypassing regulatory oversight and targeting vulnerable consumers seeking affordable or discreet medical solutions. As a result, the proliferation of these marketplaces contributes to adverse health outcomes, increased risks of drug misuse, and weakened public trust in legitimate healthcare systems.

Traditional methods for identifying illicit online pharmacies, including keyword-based filtering, block lists, and manual inspections [11], have proven insufficient in the face of evolving obfuscation tactics. Operators frequently employ subtle linguistic variations, misleading terminology, and evasive web infrastructure to avoid detection. Moreover, domain-based blocklists often lag behind the appearance of new websites, allowing malicious actors to re-emerge under different guises. These limitations highlight the need for more adaptive, scalable, and intelligent detection mechanisms.

This research investigates how Internet-wide scanning data, when combined with LLMs, can be leveraged to more effectively identify and characterize illicit online health marketplaces. Specifically, we ask: How can Internet scanning data and LLMs be utilized to detect and analyze illicit healthcare websites with greater precision and coverage? Our study addresses the following key questions and provides brief answers:

1. **How effective are existing domain/IP blocklists at detecting illicit online pharmacies?**
   Both generic and specialized blocklists each detect under 1% of candidate hosts extracted from Censys scans, offering almost no practical protection.

2. **Which keyword strategies yield the best balance between recall and precision when filtering Censys scan data?**
   Core drug names and their common misspellings (e.g., “viagra”, “cialis”) cover the most ground—our top 9 terms flag between 1,153 and 1,752 domains—while transactional phrases like “discreet shipping” or “bulk discount” further boost detection.

3. **What gains does LLM-driven query expansion deliver over manual keyword filtering?**
   LLM-generated queries uncover 6,432 hosts missed by the manual list—expanding the candidate set nearly fivefold—albeit with a modest reduction in precision.

4. **What hosting and geographic patterns do confirmed illicit pharmacies exhibit?**

Illicit sites overwhelmingly reside on cloud providers (AWS/AS16509 alone hosts 29%), with 33% based in the U.S. and 20% in India.

To address these questions, we begin by constructing a keyword list derived from prior research and known illicit pharmacy terminology. [11] Using these terms, we query Censys' Internet scanning platform to extract domain and IP data potentially linked to suspicious marketplaces. We then apply LLMs to expand and adapt the keyword set, capturing linguistic variations and discovering new candidate sites missed by the initial queries. Finally, we analyze the hosting patterns, Autonomous System Numbers (ASNs), and geographical locations of identified domains to uncover infrastructural trends used by illicit actors. Our goal is to demonstrate that pairing Internet-scale data collection with modern language models provides a powerful framework for detecting and understanding the digital ecosystem of unauthorized online pharmacies.

2 Related Work

An extensive body of work studying online anonymous markets has provided us with substantial insights into market economics, including online health platforms [2, 9]. The online pharmacy market has grown dramatically from $29.35 billion (2014) to $128 billion (2023), with research indicating approximately 95% of websites selling prescription drugs operate illegally. These illicit marketplaces span traditional websites, dark web platforms, and social media, selling prescription drugs without prescriptions, controlled substances, and counterfeit medications [19] Studies of internal databases leaked from major illicit pharmacy affiliate programs revealed that erectile dysfunction medications accounted for the most revenue in some networks, while pain medications generated substantial revenue in others. Although hosted primarily in Russia, 97% of sales occurred in the United States, Europe, Canada and Australia, with modest overall profit margins under 20% [1, 13].

Traditional approaches to identifying IOPs have relied on keyword-based filtering, as keywords containing drug names drive significant traffic to these sites. However, this approach faces several limitations: (1) the vast number of drug-related keywords makes comprehensive monitoring difficult [19]; (2) operators continuously adapt terminology to evade detection; (3) keyword filtering struggles with contextual understanding, leading to false positives and negatives [12]; and (4) illicit marketplaces have migrated to less regulated spaces like social media, complicating monitoring efforts [10].

Domain blocklists represent another approach, with organizations like the National Association of Boards of Pharmacy developing tools to identify illicit pharmacy websites. Despite their utility, these blocklists face limitation that illicit sites frequently change domains to evade detection Digital danger [3].

Also, extensive research has been conducted on the various tactics, the tactic employed by adversaries to manipulate search engine results and inject promotional content into websites. These tactics include key word stuffing [6], semantic-inconsistency techiniques [7], link farm spam [18], search redirection [5], and cloaking malicious pages with benign webpages containing commonly searched keywords [4] [17].

Recent advances in LLMs offer promising approaches for identifying illicit marketplaces. Researchers are exploring LLM applications to extract structured information from unstructured text and identify suspicious patterns [14]. Despite these advances, challenges remain, including LLM safety mechanisms that may restrict processing illegal content-related information and concerns about potential misuse to generate sophisticated fraudulent content. In our work, we are trying to utlize the creativity of LLMs to ensure more keywords coverage.

3 Methodology

In our methodology, we began by constructing two complementary Censys query strategies to identify potential illicit-online-pharmacy (IOP) hosts. First, we executed a manual keyword–based query using a curated list of "no prescription" phrases (e.g., "no prescription required," "no doctor visit") and controlled-substance terms (e.g., "xanax," "viagra"). In parallel, we prompted a large language model to synthesize these and additional indicative patterns into a single, LLM-generated CenQL query, capturing variants that manual filters might miss. Each query was submitted to the Censys API, yielding a pooled candidate set of hosts.

For each candidate host, we applied a two-pronged verification approach: candidates were either checked against trusted blocklists or subjected to LLM-based classification. For the latter, we retrieved the HTTP response body and submitted it as a contextual prompt to the LLM (Refer to Appendix 7 see prompt 2), asking it to classify the site as a genuine IOP or not. Only hosts that passed blocklist verification or were positively classified by the LLM were included in the final list. By combining manual and LLM-driven retrieval with this rigorous dual-verification process, our pipeline ensures zero false positives, balancing both precision and recall for robust detection of illicit pharmacy operations.

3.1 Blocklists

The appearance of IOPs on blocklists can serve as a potential metric for confirming their illicit nature or identifying newly discovered IOPs. In this paper, we referenced eight blocklists: three IOP-specific blocklists (snapshots of pharmacy.safe at two different points in time and FDA warning

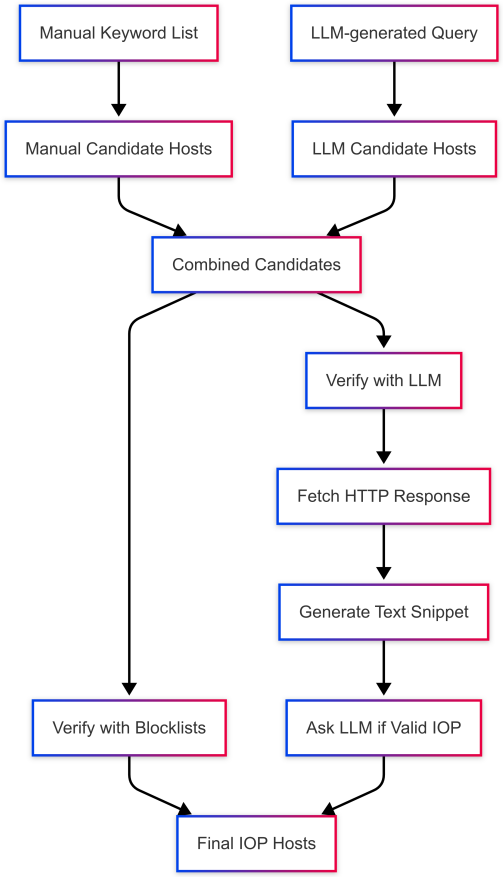

Figure 1: **Block Diagram Illustrating the Two Query Paths –** (manual keywords and LLM-generated), how their results merge into candidate hosts, and the subsequent steps of verification to yield final IOP hosts with zero false positives.

letters) and five blocklists commonly used for general protection against malicious sites (firehol_level1, blocklist_de, blocklist_net_ua, botscout_30d, and spamhaus_drop). While the IOP-specific blocklists contained DNS names, the other blocklists consisted of IP addresses to be avoided. For the context of this paper, we assume that these blocklists are a ground truth source for classifying potential websites as IOPs.

The contents of the pharmacy.safe blocklist were obtained from [15] by scraping the website using BeautifulSoup. The general blocklists were acquired from [16], where they were available for download in YAML format. The presence of an IOP in a blocklist was determined by directly matching DNS or IP addresses.

As an alternative to blocklists, one whitelist, the list of approved pharmacies compiled by National Association of Boards of Pharmacy (NAPB) was also analyzed to detect how many false positives might be resulting from the Censys keyword list query.

3.2 Keyword Frequency Analysis

To further investigate the key phases frequency results, we shifted from counting total keyword occurrences to measuring domain-level presence, because our ultimate goal is to flag illicit pharmacy websites, and it matters whether a term appears on a site at all (coverage) more than how many times it appears. By counting the number of distinct domains containing each term, we obtain a more faithful measure of a keyword's utility in real-world scanning.

3.2.1 Domain Filtering

We rely on the comprehensive NABP "Not Recommended" list as our ground truth. An initial list of candidate domains was and deduplicated to yield N unique hostnames. Each hostname was probed via HTTPS GET with a 10s timeout; only responses returning HTTP 200 (OK) were retained. All successfully validated domains were recorded to document the final analysis set and ensure reproducibility.

3.2.2 Homepage Retrieval

For each validated domain, the homepage HTML was fetched using the Python `requests` library (timeout 10s). Responses were checked for a `Content-Type` header indicating `text/html` before further processing; non-HTML responses were discarded.

3.2.3 Text Extraction

Fetched HTML was parsed with BeautifulSoup to remove all `<script>` and `<style>` elements. Visible text nodes were concatenated into a single plaintext corpus per domain,

eliminating boilerplate and markup noise so that only user-facing content contributed to subsequent counts.

3.2.4 Keyword Matching

Two keyword categories were defined as **Predefined keywords** and **Pure AI-Generated keywords**. Each term was lowercased and compiled into a case-insensitive regular expression enforcing whole-word boundaries. Each domain corpus was scanned against the full set of M patterns, and non-overlapping matches were counted.

3.2.5 Aggregation and Visualization

Per-domain counts were written in a csv file, with domains as rows and keywords as columns. The aggregate frequencies were calculated by adding the counts in all domains.

4 Results

In this section, we quantify the results of using LLMs to expand our search for IOPs. With the newly identified IOPs, we evaluate the accuracy of the results by comparing them to existing blocklists and by utilizing LLMs to assess the effectiveness based on the website's HTML content. We also analyze the effectiveness of specific keywords identified by the LLMs, highlighting trends in which keywords are the most effective.

4.1 Blocklists

Existing blocklists provide almost no protection against IOPs. As shown in Figure 2, widely used non-IOP blocklists (firehol_level1, blocklist_de, blocklist_net_ua, botscout_30d, spamhaus_drop) did not identify almost any IOPs from the candidates found by both manual and LLM-enhanced search. IOP-specific blocklists (snapshots of pharmacy.safe at two different points in time and FDA warning letters) detected some entries, but only at a relatively low rate of less than 1%. Additionally, no entries were found in the National Association of Boards of Pharmacy (NAPB) whitelist, indicating no false positives. Given the current state of existing blocklists, none are suitable for completely protecting users against IOPs.

While the low detection rates highlight the need for better IOP detection systems, existing blocklists and whitelists cannot serve as an effective metric for confirming the illicit nature of IOPs or identifying whether an IOP is newly discovered in our pipeline. The lack of detection by IOP-specific blocklists may also be a result from the dynamic nature of IOPs. To the best of our knowledge, there are no existing IOP-specific blocklists that sufficiently update regularly, which could be an effective addition to improving public safety on the internet.

Finding 1

Current internet security mechanisms fail to protect users from rogue pharmacy websites, with even specialized filters missing over 99% of these illicit operations

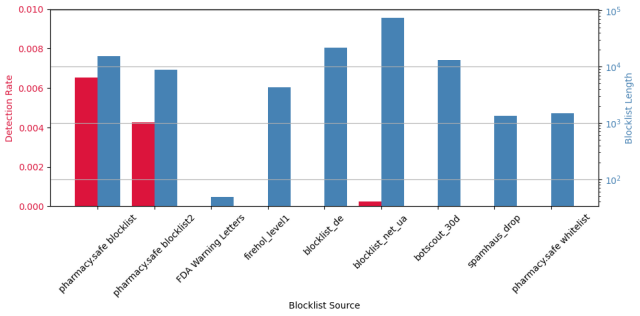

Figure 2: **Overlap with Existing Blocklists –** The combined 8431 IOP candidates from both manual and LLM-enhanced search showed virtually no overlap with widely used domain blocklists. Even IOP-specific blocklists failed to detect most IOPs, achieving a detection rate of less than 1%.

4.2 LLM Generated keywords v.s. Human Defined Keywords

Keywords Coverage Analysis. As illustrated in Section 3, our keywords combined the keywords generated using LLM, and human defined keywords. After using three LLMs (including OpenAI GPT-4o, Claude 3.7 Sonnet, and Gemini-2.0-Flash) to directly generate the keywords (Refer to Appendix 7 see prompt 1), we generated 71 unique keywords, among which 24 yielded no unique websites. As shown in the Figure 3, after refining, the keywords yield more unique websites. The data reveals significant disparities in effectiveness across different search terms. Keywords such as "no prescription," "bulk discount," and "discreet shipping" yielded the highest number of unique sites (approximately 100 each), suggesting these terms are particularly effective at identifying illicit pharmacies that evade standard detection methods. Mid-range effectiveness was observed with terms like "tramadol," "viagra," and "overnight delivery" (60-80 unique sites). Notably, certain substance-specific terms like "oxycodone" and "clonazepam" showed moderate effectiveness (approximately 70-75 unique sites), while generic terms such as "usa pharmacy" and "rx online" demonstrated relatively lower effectiveness (fewer than 20 unique sites).

Query Coverage Comparison. To evaluate how our retrieval strategies complement one another, we compared the candidate sets returned by the manual keyword–based

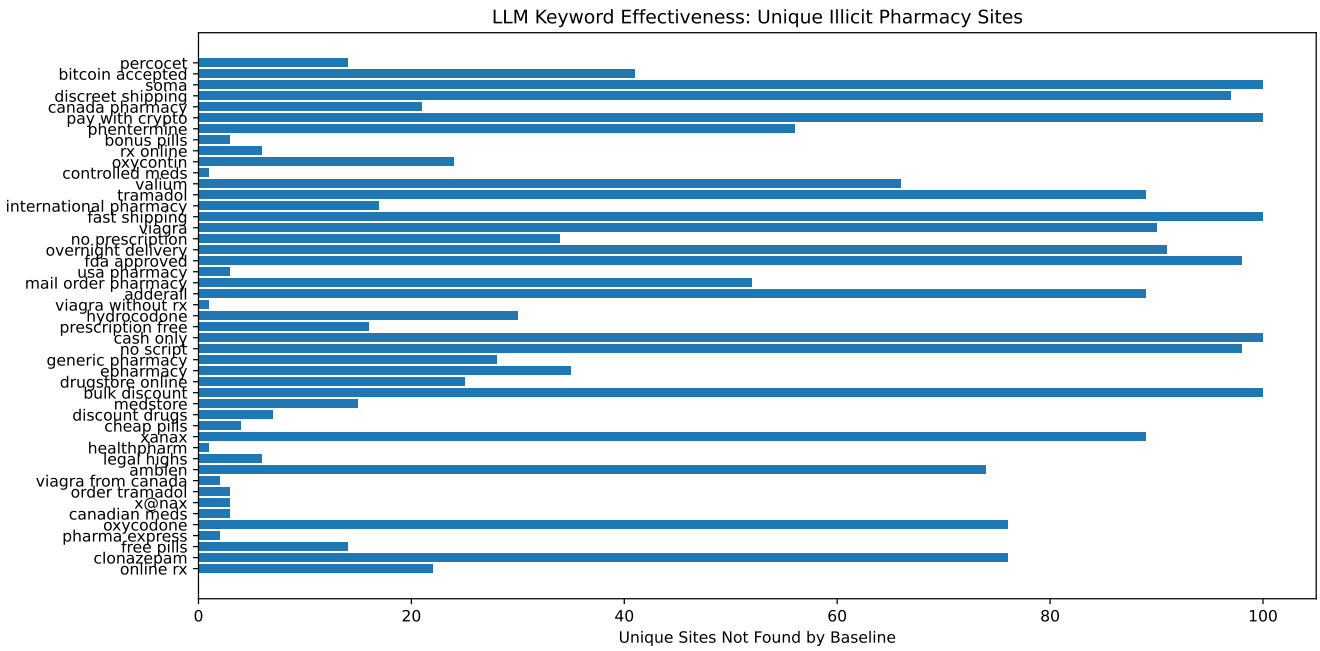

Figure 3: **LLM Keywords Effectiveness –**the number of unique illicit pharmacy sites found by different search keywords that were not detected by baseline methods. Keywords like ”discreet shipping,” ”pay with crypto,” and ”prescription free” were most effective at discovering new sites (approaching 100 unique finds each), while more specific terms like ”order tramadol” and ”canadian meds” found fewer additional sites.-

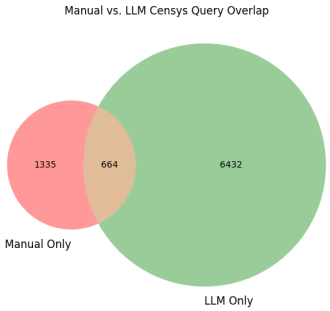

Figure 4: **IOP Candidates Source –** Comparison of IOP hosts identified using a manual keyword list query and an LLM-augmented query. The LLM-only set contains 6432 hosts, the manual-only set contains 1335 hosts, and 664 hosts were detected by both methods.

query and the LLM-augmented query (Figure4). The LLM-driven approach identified 6432 hosts that were not captured by the manual filters, whereas the hand-crafted keyword list returned 1335 unique hosts; 664 hosts were detected by both methods. This distribution demonstrates that the LLM-generated query substantially expands the search space—yielding nearly five times more unique candidates—while the manual query still contributes a distinct subset of valuable hits. Together, they offer a more comprehensive coverage of potential IOP domains than either method alone.

Candidates Screening Outcomes. Figure 5 shows the breakdown of our 8186 Censys-derived candidate sites, of which 245 were confirmed as genuine illicit online pharmacies. When stratified by discovery method, the manual keyword list (“Manual Only”) yielded the largest share of true positives, followed by sites captured exclusively by the LLM-generated query (“LLM Only”), with a smaller overlap set discovered by both approaches. This confirms that while the LLM query expands recall, our hand-crafted filters remain the most precise in isolating real IOPs.

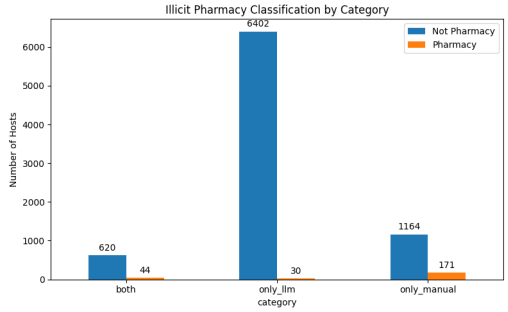

Figure 5: **Candidate Screening Results –** Results of screening 8186 Censys-derived candidates for illicit online pharmacies (IOPs). Of these, 245 sites were confirmed as real IOPs. Bars are grouped by how each site was first discovered—"Manual Only" (identified via the hand-crafted keyword list), "LLM Only" (found only by the LLM-generated query), and "Both" (captured by both methods).

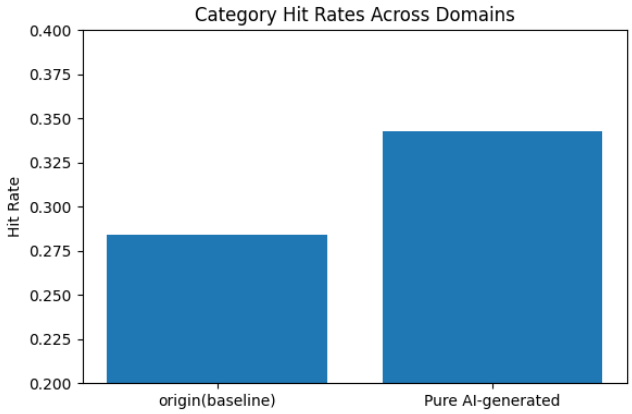

Figure 6: **Keywords Hit Rate –** Comparison of manual and AI generated keyword coverage in the NABP not recommanded website list. AI - generated key word has broader coverage than the original key word List.

Finding 2

Search queries containing terms related to discreet transactions, bulk purchasing, and prescription-free access (e.g., "discreet shipping", "bulk discount") significantly outperform baseline detection methods.

4.3 Keyword Frequency Analysis

Keyword Coverage Comparison. We evaluated the coverage of three keyword sets—(1) the original predefined keywords (baseline) and (2) the pure AI-generated keywords—by measuring how many of the $N = 7{,}794$ validated "Not Recommended" domains were flagged by each set. Figure 6 summarizes the results.

The baseline keyword set flagged 2,216 domains, corresponding to a hit rate of 28.43 %. Augmenting with AI-generated synonyms yielded only a marginal increase to 2,224 hits (28.53 %), an improvement of just 0.10 percentage points. In contrast, the pure AI-generated set matched 2,673 domains (34.30 %), representing a 5.87 pp absolute gain over the baseline and a relative increase of approximately 6 %. However, even with the AI-generated keyword list, overall coverage remains below 50 %. Examination of the sites that evaded detection reveals that an English-only keyword strategy cannot encompass the full diversity of illicit pharmacies, many of which operate in other languages. Accordingly, we confine our analysis to coverage metrics.

These findings indicate that while manually curated synonyms add little additional coverage beyond the original keyword list, the AI-generated variants capture substantially more domain-level signals. Consequently, incorporating pure AI-generated terms can meaningfully enhance the detection of illicit pharmacy sites without materially increasing false-positive volume.

Keyword Coverage Comparison. We next examined the top 30 keywords by domain coverage (Figure 7), categorizing them into three broad classes:

1. **Substance names and their orthographic variants** (e.g. brand names, misspellings),
2. **Operational/payment terms** (e.g. "western union", "btc accepted"),
3. **Prescription-requirement phrases** (e.g. "without prescription").

Drug-related terms overwhelmingly dominate the keyword list. The top nine entries correspond to erectile-dysfunction medications—"viagra" (1,752 domains), "cialis" (1,633), "sildenafil" (1,473), "tadalafil" (1,386), "levitra" (1,369), "kamagra" (1,326) and "vardenafil" (1,153)—while two high-volume orthographic variants of central nervous system stimulants and opioids, "adderal" (1,456) and "perc0cet" (1,439), complete the ranking. This pronounced concentration demonstrates that pharmaceutical substance names—and their common misspellings—provide the most salient signals for identifying illicit-pharmacy sites. Moreover, the LLM's generation of misspellings such as "adderal" and "perc0cet" highlights its ability to anticipate orthographic variants and thereby broaden detection coverage.

Mid-rank keywords (positions 11–20) reveal that misspellings of less ubiquitous drugs (e.g. "sub0xone" at 493 and "m0rphine" at 358) still contribute non-trivial coverage. In contrast, operational/payment markers such as "western union" (274 domains), "epharmacy" (270), "rx" (265), and

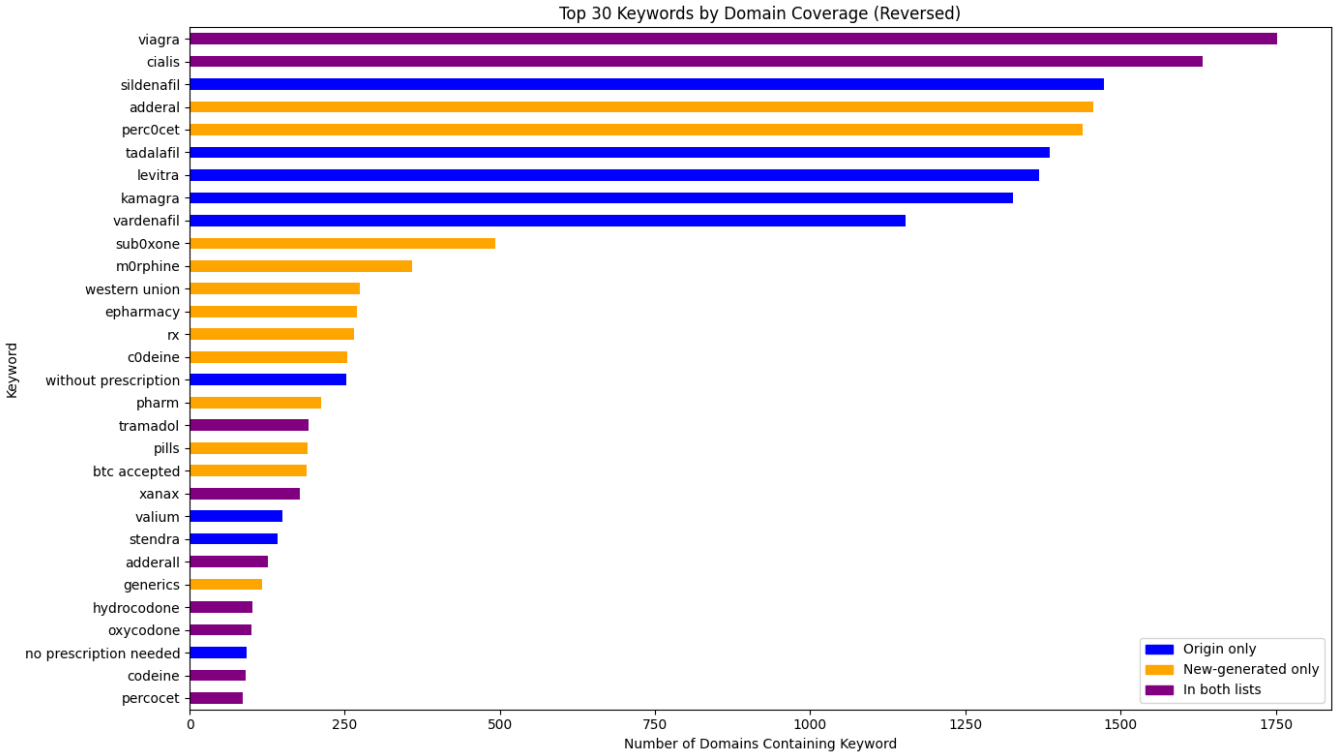

Figure 7: **Keyword Coverage Comparison –** Comparison of domain-level coverage for the top 30 keywords across the $N = 7{,}794$ validated "Not Recommended" domains. "Origin only" indicate the word from manual word list, "New- only" The substance-name and variant category (e.g. "viagra", "cialis") covers 1,153–1,752 domains, the operational/payment terms (e.g. "western union", "btc accepted") cover 189–274 domains, and the prescription-requirement phrases (e.g. "without prescription", "no prescription needed") cover up to 252 domains.

"btc accepted" (189) appear less frequently, suggesting they are weaker stand-alone indicators despite their conceptual relevance to unregulated sales.

Finally, prescription-requirement phrases—"without prescription" (252 domains) and "no prescription needed" (92)—along with generic pharmacy terms ("pharm" at 212) and packaging/shipping words ("pills" at 190), occupy lower ranks, indicating limited incremental coverage.

Finding 3

Drug name mentions—especially for high-demand medications and their common misspellings—are the most effective lexical features for flagging illicit pharmacy domains, while broader marketing or operational terms provide only modest additional reach.

4.4 Registration Information

To understand the infrastructure characteristics and evasion patterns of illicit online pharmacies, we analyzed domain registration information, hosting patterns, and network characteristics of the IOPs identified through our methodology. Using Censys data enrichment capabilities, we examined autonomous system numbers (ASNs), geographic distribution, and domain registration patterns of the 245 confirmed IOPs in our dataset.

Geographic Distribution. Utilizing Censys location data, we mapped the geographic distribution of IOP hosting infrastructure. As shown in Figure 8, the United States dominating as the primary hosting location for approximately 80 IOPs representing roughly 33% of the total, followed by India with approximately 50 IOPs representing about 20% of the total. The Netherlands hosted approximately 20 IOPs accounting for roughly 8% of the total, while Singapore hosted approximately 15 IOPs representing about 6% of the total. Australia, Canada, Germany, and the United Kingdom each hosted approximately 6-8 IOPs, representing roughly 2.5% each, while Moldova and Malaysia each hosted approximately 4 IOPs, representing about 1.5% each.

Autonomous System Number (ASN) Analysis. Network-level analysis using Censys data revealed significant concentration within specific autonomous systems (Figure 9). The top 10 ASNs accounted for approximately 60% of all IOP hosting, with Amazon Web Services infrastructure dominating the landscape. AMAZON-02 (AS16509) hosted over 70 IOPs representing approximately 29% of the total, while AMAZON-AES (AS14618) hosted an additional 25 IOPs representing roughly 10% of the total. DigitalOcean's infrastructure (AS14061) and the European hosting provider SOLLUTIUM-NL (AS60404) each hosted

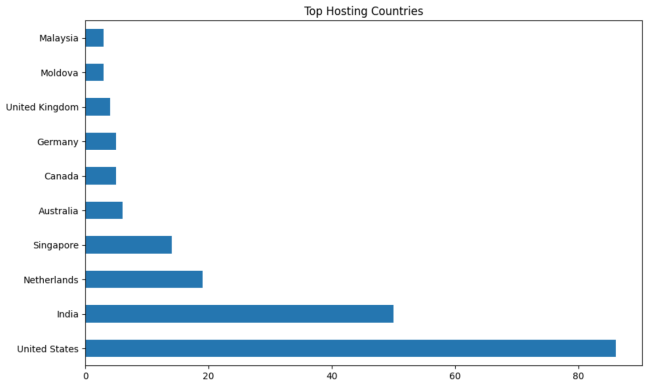

Figure 8: **Geographic Distribution of Illicit Online Pharmacy Hosting Infrastructure –** United States and India as the dominant hosts of illicit online pharmacy infrastructure

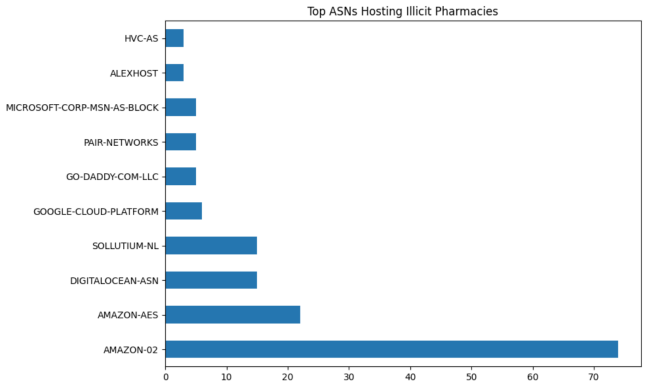

Figure 9: **Top 10 ASNs Hosting Illicit Online Pharmacies –**Amazon-O2 as the dominant Autonomous System Number (ASN) hosting illicit pharmacy sites at approximately 70 units, followed by Amazon-AES at around 22 units, with other providers including DigitalOcean, Sollutium-NL, and major cloud platforms showing significantly lower concentrations.

approximately 18 IOPs, accounting for roughly 7% each. Google's cloud services (AS15169) hosted approximately 8 IOPs, representing about 3% of the total.

Finding 4

Cloud infrastructure dominates illicit online pharmacy hosting, with the United States (33%) and India (20%) hosting over half of all IOPs.

5 Discussion

Despite careful query design and the use of both manual and LLM-generated patterns, our methodology yields a substantial number of false positives when identifying illicit online

pharmacy (IOP) hosts. This issue primarily stems from several factors:

First, there is the inherent ambiguity of language and the widespread use of medical and pharmaceutical terms in legitimate contexts. Many health information portals, news articles, patient forums, and regulatory websites frequently mention controlled substances or prescription-related keywords, which can trigger our candidate selection process even though these sites lack any illicit sales activity. The LLM classifier, while powerful, can also misinterpret the intent or context of such mentions, especially in cautionary or informational articles that warn against unauthorized drug sales or educate consumers about pharmaceutical risks.

Second, limitations in live data retrieval introduce another source of false positives. Our pipeline relies on Censys queries to identify hosts based on historical scan data, which reflect the state of the host at the time of the scan, not necessarily at the time of our verification. When we attempt to fetch live HTTPS responses from these candidate IPs, we frequently encounter failures—such as 404 errors, empty responses, or content mismatches. These issues arise because the original content may have been removed or altered, the host may now be inactive, or the server configuration (e.g., reliance on virtual hosting or SNI) prevents access to the expected page via a direct IP request. Additionally, some hosts block or rate-limit automated queries, further complicating real-time verification.

Finally, the broad reach of our initial candidate queries—particularly those generated by the LLM—magnifies these effects. Our results show that the LLM-augmented query substantially broadens the search space for potential IOP hosts, identifying nearly five times more unique candidates than the manual keyword list alone. This expansion likely arises from the LLM's ability to infer synonyms, contextual cues, and novel phrasings outside the scope of hand-crafted filters, enabling it to capture emerging or obfuscated illicit-pharmacy signals. However, this comes at the cost of precision: a larger fraction of LLM-only hosts are false positives compared with those retrieved solely by manual keywords.

Together, these factors highlight the persistent challenge of balancing recall and precision in automated IOP detection. While the LLM query excels at recall, its precision can be further improved—perhaps by refining prompts, incorporating domain-specific constraints, or retraining on a curated IOP corpus. In practice, combining the strengths of both approaches—using the manual list to filter high-confidence hits and the LLM query to expand coverage—yields a more balanced pipeline. Future work will focus on optimizing this hybrid strategy, including dynamic weighting of query components, enhancing verification mechanisms for candidate hosts, and developing iterative feedback loops between LLM outputs and manual rule updates.

6 Conclusion

In this work, we systematically explored the detection of illicit online pharmacy (IOP) hosts using a hybrid methodology that leverages both manual keyword queries and large language model (LLM)-generated search patterns. By integrating traditional, hand-curated keyword strategies with advanced LLM-driven query expansion and classification, we demonstrated that our approach dramatically broadens the coverage of candidate IOP hosts—uncovering a far larger pool of potentially illicit domains than conventional methods alone.

Our results reveal several key insights. First, existing blocklists, including those specifically targeting IOPs, offer almost no protection against the evolving threat landscape posed by rogue pharmacy sites. The LLM-augmented queries, while significantly increasing recall by surfacing more candidates, also introduce a greater risk of false positives due to the ambiguity of language and the diverse contexts in which medical terms are discussed online. In-depth analysis of keyword effectiveness underscores that substance names and their variants are the most reliable lexical signals for identifying IOPs, while broader operational or marketing terms provide only marginal additional coverage.

Despite these advances, challenges remain in striking an optimal balance between recall and precision. Limitations inherent in live data retrieval, the dynamic nature of web content, and the tendency of LLMs to surface ambiguous results all highlight the need for more sophisticated verification and filtering mechanisms. Our dual-verification approach—using blocklists and LLM-based content analysis—serves as a practical step forward, but further refinements, such as more targeted LLM prompts, domain-specific training data, or adaptive hybrid filtering strategies, are necessary to minimize false positives without sacrificing coverage.

Looking ahead, future work will focus on enhancing the robustness and adaptability of IOP detection pipelines. Promising directions include the dynamic weighting of manual and LLM-generated query components, automated feedback loops for iterative rule and model refinement, and the incorporation of richer contextual signals (such as temporal patterns or network behavior) into the classification process. Ultimately, our findings demonstrate that LLMs, when thoughtfully combined with expert knowledge and systematic validation, can play a pivotal role in the ongoing effort to safeguard public health and online safety from the risks posed by illicit pharmacy operations.

7 Contribution

Yufei Song. Yufei developed a robust pipeline that integrates both manual and LLM-generated Censys queries with LLM verification to ensure zero false positives, enabling

comprehensive and precise detection of illicit online pharmacy hosts. Yufei compared the results from LLM and manual keyword query, analyzed the results and dicussed future improvements on the methodology for identifying IOPs more precisely.

Ying Li. Ying conducted the comprehensive literature review for Section 2 (Related Work), led the infrastructure analysis in Section 4.4 (Registration Information) using Censys data to examine domain registration patterns, ASN distributions, and geographic hosting characteristics, and designed the comparative evaluation between LLM-generated and manually curated keyword coverage to assess their effectiveness in IOP detection.

Taiga Asanuma. Taiga developed the pipeline for identifying the overlap between manual and LLM-generated Censys results against three IOP blocklists, five non-IOP blocklists, and one IOP whitelist. Taiga analyzed the results, confirming the current limitations on existing blocklists. Taiga was also responsible for the abstract.

Zihan Wang. Zihan extracted the NABP "Not Recommended" list from its online source and curated it into a validated illicit-pharmacy domain set. Zihan designed and implemented the end-to-end pipeline for measuring domain-level keyword frequency—covering HTTPS retrieval, HTML parsing, text extraction, and regex-based matching across three keyword categories. Finally, Zihan conducted the statistical analysis comparing predefined keywords and AI-generated variants, produced the coverage metrics and visualizations, and drafted the corresponding Results subsection.

References

[1] Valeria Catalani, Honor D Townshend, Mariya Prilutskaya, Robert P Chilcott, Antonio Metastasio, Hani Banayoti, Tim McSweeney, and Ornella Corazza. Illicit covid-19 products online: A mixed-method approach for identifying and preventing online health risks. *Plos one*, 18(6):e0287231, 2023.

[2] Alejandro Cuevas, Fieke Miedema, Kyle Soska, Nicolas Christin, and Rolf van Wegberg. Measurement by proxy: On the accuracy of online marketplace measurements. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 2153–2170, 2022.

[3] Ahmed Ghappour. Searching places unknown: Law enforcement jurisdiction on the dark web. *Stan. L. Rev.*, 69:1075, 2017.

[4] Luca Invernizzi, Kurt Thomas, Alexandros Kapravelos, Oxana Comanescu, Jean-Michel Picod, and Elie Bursztein. Cloak of visibility: Detecting when machines browse a different web. In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 743–758. IEEE, 2016.

[5] Nektarios Leontiadis, Tyler Moore, and Nicolas Christin. Measuring and analyzing {Search-Redirection} attacks in the illicit online prescription drug trade. In *20th USENIX Security Symposium (USENIX Security 11)*, 2011.

[6] Xiaojing Liao, Chang Liu, Damon McCoy, Elaine Shi, Shuang Hao, and Raheem Beyah. Characterizing long-tail seo spam on cloud web hosting services. In *Proceedings of the 25th International Conference on World Wide Web*, pages 321–332, 2016.

[7] Xiaojing Liao, Kan Yuan, XiaoFeng Wang, Zhongyu Pei, Hao Yang, Jianjun Chen, Haixin Duan, Kun Du, Eihal Alowaisheq, Sumayah Alrwais, et al. Seeking nonsense, looking for trouble: Efficient promotional-infection detection through semantic inconsistency search. In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 707–723. IEEE, 2016.

[8] Yam B. Limbu and Bruce A. Huhmann. Illicit online pharmacies: A scoping review. *International Journal of Environmental Research and Public Health*, 20(9), 2023.

[9] Yam B Limbu and Bruce A Huhmann. Illicit online pharmacies: a scoping review. *International Journal of Environmental Research and Public Health*, 20(9):5748, 2023.

[10] Tianyi Ma, Yiyue Qian, Zehong Wang, Zheyuan Zhang, Chuxu Zhang, and Yanfang Ye. Llm-empowered class imbalanced graph prompt learning for online drug trafficking detection. *arXiv preprint arXiv:2503.01900*, 2025.

[11] Tim Mackey, Janani Kalyanam, Josh Klugman, Ella Kuzmenko, and Rashmi Gupta. Solution to detect, classify, and report illicit online marketing and sales of controlled substances via twitter: Using machine learning and web forensics to combat digital opioid access. *J Med Internet Res*, 20(4):e10029, Apr 2018.

[12] Tim K Mackey and Gaurvika Nayyar. Digital danger: a review of the global public health, patient safety and cybersecurity threats posed by illicit online pharmacies. *British medical bulletin*, 118(1):110–126, 2016.

[13] Damon McCoy, Andreas Pitsillidis, Jordan Grant, Nicholas Weaver, Christian Kreibich, Brian Krebs, Geoffrey Voelker, Stefan Savage, and Kirill Levchenko.

{PharmaLeaks}: Understanding the business of online pharmaceutical affiliate programs. In *21st USENIX Security Symposium (USENIX Security 12)*, pages 1–16, 2012.

[14] Maximilian Mozes, Xuanli He, Bennett Kleinberg, and Lewis D Griffin. Use of llms for illicit purposes: Threats, prevention measures, and vulnerabilities. *arXiv preprint arXiv:2308.12833*, 2023.

[15] National Association of Boards of Pharmacy. Not recommended sites. Accessed: 2025-05-11.

[16] Costa Tsaousis. Firehol ip lists. Accessed: 2025-05-11.

[17] David Y Wang, Stefan Savage, and Geoffrey M Voelker. Cloak and dagger: dynamics of web search cloaking. In *Proceedings of the 18th ACM conference on Computer and communications security*, pages 477–490, 2011.

[18] Baoning Wu and Brian D Davison. Identifying link farm spam pages. In *Special interest tracks and posters of the 14th International Conference on World Wide Web*, pages 820–829, 2005.

[19] Hui Zhao, Sowmyasri Muthupandi, and Soundar Kumara. Managing illicit online pharmacies: web analytics and predictive models study. *Journal of medical Internet research*, 22(8):e17239, 2020.

Appendix

7.1 Used Prompts

Prompt 1 The prompt used to generate Censys Query Keywords

You are a cybersecurity researcher investigating illicit online pharmacies. Your goal is to generate a comprehensive list of keywords that are commonly used by rogue or unlicensed pharmacy websites and can help identify them using Censys search queries. These keywords are likely to appear in:

- Domain names (e.g., cheapviagrapills.com, fastmeds247.net)
- TLS/SSL certificate fields (e.g., Common Name, Subject, SANs)
- HTTP service banners or metadata (e.g., server title, description, or headers)
- WHOIS information (e.g., organization name, contact email)

Your keyword list should focus on indicators of illegal or unregulated operations and exclude terms likely used only by legitimate pharmacies. Please consider the following categories:

- Common drug names and misspellings — e.g., addictive or controlled substances often sold illegally (e.g., viagra, xanax, tramadol, plus misspellings like v1agra, x@nax).
- Pharmacy-related terms — terms that frequently appear in illegal pharmacy branding or infrastructure (e.g., rx, pharma, drugstore, medsonline).
- Suspicious marketing claims — phrases emphasizing ease of access or price, often used by rogue sellers (e.g., no prescription, cheap pills, FDA approved without context).
- Shady business practices — signs of illegitimacy, such as unusual payment methods or shipping terms (e.g., bitcoin accepted, overnight delivery, bulk discount).
- Geolocation-based clues — country labels misused to suggest legitimacy or to obscure regulation (e.g., canada pharmacy, international meds).

  Output format: Return a JSON array of lowercase strings. Each string should be a keyword or phrase (exact match or common variant) that is likely to be used by an illicit pharmacy.

Prompt 2 The prompt used to determine whether it is a real Illicit Online Pharmacy or not

Classify this site as Illicit Online Pharmacy or not using exactly this JSON schema:
{
”is_pharmacy”: boolean,
”confidence”: number,
”reason”: string
}
”Host: {host}
Title: {title}
Snippet: {text[:3000]}