# ChatScam: Unveiling the Rising Impact of ChatGPT on Domain Name Abuse

Mingxuan Liu*, Zhenglong Jin†, Jiahai Yang‡, Baojun Liu†✉,
Haixin Duan†*✉, Ying Liu†*, Ximeng Liu‡, Shujun Tang§

*Zhongguancun Laboratory, China †Tsinghua University, China
‡Fuzhou University, China §QI-ANXIN Technology Research Institute, China
liumx@mail.zgclab.edu.cn, jzl23@mails.tsinghua.edu.cn, 231027027@fzu.edu.cn,
{lbj, duanhx}@mail.tsinghua.edu.cn, liuying@cernet.edu.cn, snbnix@gmail.com, tangshujun@qianxin.com

***Abstract*—Since 2022, ChatGPT has been a big breakthrough in technology, creating lots of discussions online. It has had big effects in different areas, but in cybersecurity, it is both good and bad. There has been a lot of misuse, especially with squatting domains. Our research aims to understand this misuse and the potential threats it poses. We develop a novel method that looks at historical Passive DNS (PDNS) data. Based on the two-stage identification, our method can efficiently and accurately collect ChatGPT-related squatting domains. In the end, we found over 1.3 million ChatGPT-related squatting domains, part of which were shared with the security community. Our findings show that these squatting domains are increasing quickly. This is the case whether the keywords related to ChatGPT are registered with the domain registrar or set up on subdomains. Even though the number of domains is increasing, only 5.3% set up meaningful content on their websites. After digging into their web contents, we found that these websites show various signs of misuse, such as promotion on illegal underground websites and emerging fraudulent activities related to dialogue features. The security community is not fully aware of these threats yet. We are the first to conduct a large-scale quantitative analysis of ChatGPT-related abusive behavior. We believe that our work unveils the abuse ecosystem surrounding ChatGPT-related squatting domains. We hope to underscore the urgent need for increased attention and protective measures against ChatGPT-related domain abuse.**

## I. Introduction

ChatGPT [65], a large-model-driven intelligent dialogue system, has sparked considerable discourse. Its advent significantly refines machine comprehension of language inputs, making automated understanding of natural language feasible. The exceptional performance of ChatGPT has radically transformed operational patterns across various sectors. Examples include enhancing search engine performance like Bing [57], generating high-quality articles [61], assisting in code debugging [21], and even ideation [64], etc.

ChatGPT has also significantly influenced cybersecurity, acting as a double-edged sword. On one hand, the intelligence substantially of ChatGPT bolsters our defenses against cyber-attacks. Researchers introduced ChatGPT-based methods for various security applications, such as identifying network device fingerprints [73], detecting phishing websites [42], and toxic content [35]. Unfortunately, the advanced abilities of ChatGPT have also been exploited by miscreants, leading to numerous abuse cases. Examples include the use of scam domains related to ChatGPT for phishing [55], websites that mimic legitimate ChatGPT plugins to steal user credentials or distribute malware [16], and social engineering attacks with the malicious version of ChatGPT [29]. Besides, the surging traffic of ChatGPT hype is widely exploited to promote illicit industries for profitable advertising [15].

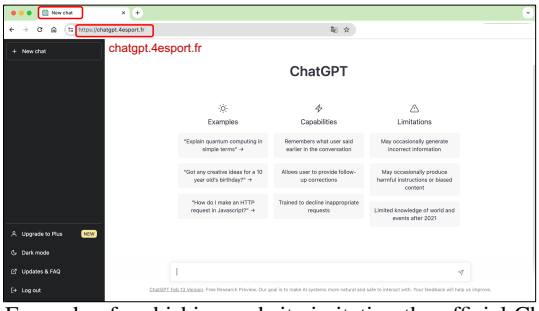


Fig. 1: Example of a phishing website imitating the official ChatGPT website.

**Motivation.** Though a few blogs have discussed individual abuse risks brought by ChatGPT [68], a comprehensive overview of the impact of ChatGPT on abuse activities in cybercrime is still missing. It is important to spot and track ChatGPT-related squatting domain names (referred to as squatting domains in this paper) in cyberspace. We believe that understanding these suspicious domains can help the security community prevent malicious ChatGPT-related activities.

**Our work.** To fully understand the impact of ChatGPT on domain abuse activities, we utilized the Passive DNS (PDNS) dataset, which could provide a comprehensive view of DNS resolution. In this work, we categorize all unauthorized squatting domain names with ChatGPT-related keywords as malicious conduct of interest in our paper based on OpenAI's official guidelines [67], including the abuse of its hype and technology. Finding ChatGPT-related squatting domain names in the huge PDNS logs is a big challenge. So, we proposed a funnel-shaped identification method based on an extensive ChatGPT-related keyword list, first using fuzzy matching to downgrade the volume of DNS logs, and then precisely matching ChatGPT-related squatting domains. Employing this method, we can efficiently and accurately identify ChatGPT-

related squatting domain names. To help future work on analyzing ChatGPT-related abuse activities, we share part of these domains publicly[1].

**Our Findings.** After an in-depth examination of these ChatGPT-related squatting domain names, we noticed these unofficially registered domains have some inherent security risks. First, the trend of embedding ChatGPT-related keywords in domain names is rapidly gaining popularity. Judging by the volume of DNS resolutions, these squatting domains indeed attract a lot of traffic. Over 31k squatting domains have received more than 1,000 DNS resolution queries. What's worrying is that, upon analyzing the keywords linked with ChatGPT, we found several squatting attack methods, including combosquatting and homograph attacks. These squatting methods significantly increase the domain space that adversaries could abuse. A large number of ChatGPT-related squatting Second-Level Domains (SLDs) have been registered through 1,072 registrars, across 445 Top-Level Domains (TLDs). Furthermore, we observed signs of bulk registration of ChatGPT-related squatting domain names. Almost half of the ChatGPT-related squatting domain names are set up as subdomains of third-party network service domains, like cloud storage *amazon-aws.com*. This greatly increases the chances for levelsquatting attacks, especially on mobile platforms. Unfortunately, nearly none of these registration and web hosting organizations have taken steps to prevent such unofficial squatting activities. This lack of action gives miscreants many opportunities to register domains and set up webpages.

**Novel Security Threats.** Through analyzing and classifying page content, we determined that 94.7% of the ChatGPT-related squatting domains have not set up any meaningful content. For example, they might be blank or only have configuration information. Even without content, some domains are parked, potentially for profit gain. Even more notable, 20.93% of ChatGPT-related squatting domains are used as promotional tools by underground industries like gambling and pornography. In these cases, ChatGPT-related keywords are embedded in the subdomains of the apex domains. ChatGPT-related keywords in illicit domains not only increase the chances that users will see them, but also increase the likelihood of users visiting the website. This abuse of ChatGPT hype breaks the official brand guidelines [67]. Besides, ChatGPT's intelligent dialogue technology is a prime target for abuse. On websites with dialogue features, we first exposed many unauthorized mirror sites of ChatGPT that do not comply with official regulations. Some of these are even phishing websites that imitate the official site exactly, as shown in Figure 1. These sites claim to offer the same services as the official ChatGPT, and use this to earn money. The strong demand for ChatGPT has thus led to an industry that is creating unauthorized ChatGPT mirror websites for profit. Unfortunately, upon cross-checking with Threat Intelligence (TI), we found that only 18% of these malicious squatting domains have been reported as harmful. This suggests a significant delay and false negatives in detecting these new abusive activities related to ChatGPT. In light of our findings, we believe that the issue of ChatGPT-related squatting domain name abuse indeed warrants increased attention from the cybersecurity community.

**Contributions.** By examining ChatGPT-related squatting domains, our main contributions are:

- *Identification method.* We propose an efficient and accurate method to efficiently and accurately identify ChatGPT-related squatting domain names from the PDNS dataset.
- *Comprehensive understanding.* From the perspective of historical DNS resolutions, we conducted the first comprehensive analysis of the ChatGPT-related squatting domain name to unveil their ecosystem and associated abusive activities. And we identified several previously undisclosed security risks.
- *Open-source dataset.* From PDNS dataset, we continuously collect and analyze ChatGPT-related squatting domains, and open source part of these domains. We believe this continuous open dataset can help the security community keep track of ChatGPT-related abuse threats over the long term.

## II. Background

In this section, we provide a brief introduction to the Domain Name System (DNS), covering the structure and creation of domain names, how domains are resolved in the DNS, and squatting techniques.

### A. Domain Name

A domain name is organized in a hierarchical structure, with levels divided by a period (“.”). For example, in *chatgpt-squatting.dsn2024.com.*, from top to bottom, these are the DNS root (the rightmost point often omitted in writing), the top-level domain (TLD) (i.e., “com”), the second-level domain (SLD) (i.e., “dsn2024.com”), and then the subdomain (i.e., “chatgpt-squatting.dsn2024.com”). The whole domain name is often called a Fully Qualified Domain Name (FQDN). The TLD is approved by ICANN and run by different registries. The SLD, also known as the apex domain, is registered by the registrant from the registrar. The domain owner can freely set up subdomains for their apex domain without needing permission from the registrar.

Originally, domain names only allowed ASCII characters. But as internationalization progressed, Internationalised Domain Names (IDNs) emerged. IDNs let registrants use non-ASCII characters, like Chinese and Japanese, in domain names, which expands the character type across all Unicode characters. To keep compatibility, domain names with non-ASCII characters have to be re-encoded into ASCII characters for resolution and further operations. This re-encoding process, called Punycode transformation, keeps all ASCII characters and encodes non-ASCII characters using variable-length integers. All domain names that undergo Punycode transformation bear a constant prefix, “xn–”.

[1] https://github.com/MingxuanLiu/ChatScam/

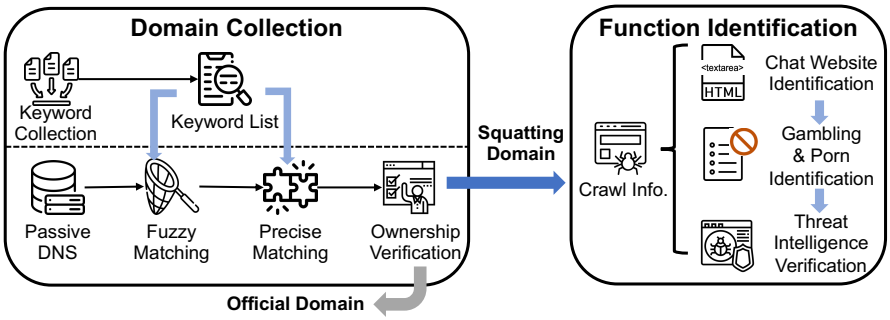



Fig. 2: The workflow of the identification system for ChatGPT-related squatting domains.

### B. Domain Name Resolution

The DNS resolution converts domain names into IP addresses. Common DNS record types include A records (IPv4 addresses), AAAA records (IPv6 addresses), CNAME records (aliases), and NS records (authoritative servers) [59, 60].

Passive DNS (PDNS) is a dataset passively collected from DNS resolution traffic (both requests and responses) from DNS resolvers. Each entry in the PDNS dataset is a six-part tuple, denoted as *<first_see, last_see, count, rrname, rrtype, rdata>*. This shows that from *first_see* to *last_see*, the domain *rrname* has been resolved to *rdata* a total of *count* times. Since the PDNS dataset encapsulates all DNS resolution traffic seen on the resolver and keeps historical records, it can reflect the resolution status of a domain name comprehensively.

### C. Squatting Technique

Domain names are often misused for harmful activities like spreading Botnets. One common method of domain abuse is squatting techniques. These methods create domain names that look very similar to authoritative ones, making it hard for victims to tell the difference between genuine and deceptive domains, thus enabling deception and fraud. For example, homograph attacks use visually similar characters from different Unicode scripts [81]. There are also other types of attacks like combosquatting [41], which combines keywords, and levelsquatting [27], which uses excessively long subdomains.

## III. Identification Methodology

In this section, we propose a method to identify ChatGPT-related domain names. First, we find domain names using a funnel-shaped matching method based on ChatGPT-related keywords. Then, we use heuristics to determine the content categories of these domains.

### A. Overview

Identifying ChatGPT-related squatting domains accurately from an extensive volume of PDNS logs presents a significant performance challenge. To address this, we present an identification methodology, shown in Figure 2, which has two main stages. First, we devise a funnel-shaped identification method. This includes character-level fuzzy matching to lessen the number of pending DNS logs, and precise matching within manageable limits. This step, which is confirmed through multiple validations, provides a set of unofficial ChatGPT-related squatting domains. Then, to analyze website content, we propose a heuristic-guided approach for inferring web intent. This process starts with a crawl for extra data, such as WHOIS, current DNS resolution results, and HTTP responses. Based on an empirical study, we divide the websites into 4 categories: chat-function providing websites, underground websites (including gambling and pornography), parking and for sale websites, and other websites.

Using our method of identifying ChatGPT-related domains, we collaborated with 114 DNS, a leading DNS service in China. They maintain an ongoing and large dataset, capturing all DNS communications observed from their public DNS resolvers. This dataset includes around 500 billion unique DNS requests daily for about 550 million FQDNs. Considering the public date of ChatGPT, we focused on data from January 2022 to August 2023. This period allows us to thoroughly understand domain name activities associated with ChatGPT in its early years.

### B. Domain Collection

Given the vast volume of PDNS logs (about 550 million per day), it is unfeasible to directly perform precise keyword matching on such an extensive dataset. To tackle this challenge, building upon existing research [50, 90], we devised a funnel-shaped matching methodology based on a grounded list of ChatGPT-related keywords. The primary philosophy of this method entails the gradual diminution of DNS logs pending processing. This approach facilitates the precise detection of ChatGPT-related squatting domains within a controllable scale, thereby enhancing efficiency.

We first gathered a set of keywords highly pertinent to ChatGPT, selected based on empirical expertise and expanded via search engine capabilities [90]. After manual verification, we selected the 4 most relevant seed keywords, i.e., *chat, gpt, open* and *ai*. Additionally, our study extends to the impact of similar intelligent conversational services on cybercrime, thus incorporating two non-OpenAI services, *claude* [6] and *copilot* [58], as keywords. Consequently, we identified 6 seed keywords. In pursuit of comprehensive coverage of related domain names, we accounted for certain squatting attack techniques, including typosquatting [2], homograph IDN [37, 48], combosquatting [41]. By leveraging an open-source software,

dnstwist [25], we could automatically generate squatting variants of seed keywords. As a result, we expanded our original keyword list to a total of 11,170 entries. Given that squatting generation introduces IDNs encoded with Punycode format, with a distinct encoding commencing with "xn–" [18]. For example, the Punycode of *cîaude.ai* is *xn–caude-5sa.ai*. Since our seed keywords can mistakenly catch unrelated words, such as "ai" in "air", but "air" is irrelevant. While the Punycode keywords, derived from seed keywords using non-ASCII characters, is less possible to form unintended words due to the "xn–" prefix, eliminating the need for additional processes to filter false positives. Consequently, we differentiated our keyword list into two subsets for efficiency based on Punycode encoding characteristics, i.e., the IDN set ($K_{puny}$) and the non-IDN set ($K_{normal}$). Moreover, there are potential false positives arising from overlaps between keywords and Chinese Pinyin or segments of prominent domains. For example, "kuai" in *kuaishou.com* represents a Chinese phonetic rendering and, despite containing the keyword "ai", is not related to ChatGPT. Besides, though *freshchat.com* contains "chat" keyword, it is an instant messaging tool rather than a representative of intelligent conversational capabilities. Therefore, to prevent these potential false positives, we created an additional keyword list based on the Chinese pinyin library with all Chinese pronounces [44] (e.g., "kuai") and a list of hierarchical levels from popular domains within the Tranco Top list [70], excluding the Top-Level Domains (TLDs) (e.g., "freshchat").

Subsequently, using this expanded keyword list, we employ a two-step process to pinpoint ChatGPT-related domains, as outlined in Algorithm 1. This process comprises *Fuzzy Matching* to reduce the quantity of DNS logs requiring processing, and *Precise Matching* to accurately distinguish ChatGPT-related squatting domains. During the *Fuzzy Matching* phase (Lines 1 to 7), we aim to extract as comprehensive a set of domain names as efficiently as possible. Therefore, we apply all keywords from the $K_{puny}$ and $K_{normal}$ directly to the complete PDNS data set for matching. Throughout this fuzzy matching process, we obtained 3,645,463,873 initial domain names. The Fuzzy Matching phase greatly diminishes the scale of the PDNS dataset. However, this process could potentially introduce certain false positives. Therefore, the subsequent *Precise Matching* process serves to filter out potential false positives and accurately identify domains related to ChatGPT (Lines 8 to 23). Specifically, since Punycode domains, precisely generated from initial keywords, are encoded from IDNs and all have the "xn–" prefix, we consider those that match the $K_{puny}$ list directly to be ChatGPT-related domains (Lines 11 to 13), not false positives. For non-Punycode domains, we initially conduct a segmentation process on the domain (Line 14) to obtain its word list, $split\_domain$. For instance, *livechat.com* is segmented into *live*, *chat*, and *com* based on English segmentation, and *kuaishou.com* is segmented into *kuai*, *shou* and *com* based on Chinese pinyin. Subsequently, we compare this with $L_{known}$, eliminating words present in $L_{known}$ (Lines 15 to 16). Finally, we assess the count of non-Punycode keywords, and deem domains with 2 or more keywords as being related to ChatGPT (Lines 17 to 19). Finally, we filter out all subdomains within the official domains (Lines 20 to 22). Our keyword selection pertains exclusively to ChatGPT and two other most prominent applications, Claude (developed by Anthropic) and Copilot (developed by Microsoft). Consequently, we confined our filtration process to 3 official websites.[2] This process ensures that identified domains are unofficial squatting domains.

**Algorithm 1:** IDENTIFYING CHATGPT-RELATED DOMAIN NAMES

**Data:** Passive DNS dataset $Q$, $q \in Q$ is a DNS record, Punycode keyword list $K_{puny}$, None punycode keyword list $K_{normal}$, Pinyin List and popular domain word list $L_{known}$
**Result:** ChatGPT-related domains $D_{chat}$

1 $Q^* \leftarrow \{\}$ ▷ Initialization of Fuzzy Matching Result
2 **foreach** $q \in \mathcal{Q}$ **do**
3  $domain \leftarrow q[fqdn]$ ▷ Get domain in DNS record
4  **if** $domain \cap K_{puny} \neq \varnothing$ or $domain \cap K_{normal} \neq \varnothing$ **then**
5  $Q^*$.append $q$ ▷ Fuzzy Matching
6  **end**
7 **end**
8 $D \leftarrow \{\}$ ▷ Initialization of Precise Matching Result
9 **foreach** $q^* \in \mathcal{Q}^*$ **do**
10  $domain \leftarrow q^*[fqdn]$
11  **if** $domain \cap K_{puny} \neq \varnothing$; **then**
12  $D$.append $domain$ ▷ Punycode Domain
13  **end**
14  $split\_domain \leftarrow \text{tokenize}(domain)$ ▷ Tokenization of None-Punycode Domain
15  $word_{known} \leftarrow split\_domain \cap L_{known}$
16  $split\_domain.remove(word_{known})$ ▷ Remove Known Words
17  **else if** $split\_domain \cap K_{normal} \geq 2$ **then**
18  $D$.append $domain$
19  **end**
20  **if** $verify\_ownvership(domain) == official$ **then**
21  $D$.remove $domain$ ▷ Remove Official Domains
22  **end**
23 **end**
24 **return** $D$

Following the Domain Collection process, we obtained ChatGPT-related squatting domains. To understand the purposes of these webpages, we designed a heuristic-based function identification method.

First, we obtained relevant auxiliary information regarding the identified ChatGPT-related domains, facilitating further processing and analysis.

• **Passive DNS records** present the historical resolution results of each domain name. We selected the relevant PDNS records associated with ChatGPT-related squatting domain names from the 114 PDNS dataset, using SLD and FQDN as criteria.

We present the identification results of the ChatGPT-related domains in Table I. In total, we identified **1,357,638 FQDNs**, which belong to **119,907 SLDs**.

### C. Function Identification

[2]Three official SLDs includes *openai.com*, *claude.ai*, and *copilot.com*.

TABLE I: Domain Collection Results.

| - | # DNS Record | # FQDN | | # SLD | |
|---|---|---|---|---|---|
| | | All | Top100k | All | Top100k |
| **Fuzzy Matching** | 4,757,013,828 | 3,645,463,873 | 1,292,026,514 | 444,547,914 | 50,401,203 |
| **Precise Matching** | 4,061,883 | 1,526,136 | 785,110 | 119,910 | 3,139 |
| **Ownership Verification** | 3,842,117 | 1,357,638 | 616,613 | 119,907 | 3,137 |
| **ChatGPT-related Domains** | | **# FQDN: 1,357,638**<br>**# SLD: 119,907** | | | |

* "Top100k" means the number of domain names whose SLD are ranked in the Top 100,000, which is collected from Tranco Top list [70].

• **WHOIS records** present the registration information of each domain name. We used a Python library to obtain and parse WHOIS information.[3] Due to privacy protection initiatives under the General Data Protection Regulation (GDPR) [52], we currently cannot access the information of domain registrants, such as their email addresses. This limitation makes it challenging to directly analyze instances of bulk registration by a single registrant.

• **Current DNS resolution** includes several basic DNS resolution types, like *A*, *NS*, *CNAME*, *MX*, and *SOA*. These DNS requests were then sent to several well-known DNS resolution servers [71] for resolution, and the responses were recorded.

• **Web contents** include HTTP responses and webpages. Specifically, we built HTTP requests and used BeautifulSoup [4] to parse the response and record specific information.

Note that, due to the lack of understanding of the ground-truth, it is challenging for us to comprehensively analyze all webpages of ChatGPT-related domains along with their content and intent. Therefore, in this study, we first conduct an empirical study for randomly sampled 300 FQDNs. Two researchers independently labeled these 300 websites. Ultimately, we identified 4 categories within all ChatGPT-related squatting domains: websites that mirrored ChatGPT with intelligent dialogue functions (10 websites), underground websites which included 29 gambling websites and 21 pornographic sites, domain parking and sale websites (98 websites) and other type (142 websites). Note that, the other type includes websites with too little text content to determine their purpose, and site-building templates (such as Nginx, Apache, etc.). By deeply analyzing the characteristics of these 4 categories of websites, we designed a four-fold cross-identification classification method. This includes the analysis of key HTML tags related to Chat functionality, textual content analysis associated with the common underground industry (mainly including gambling and porn websites), name server analysis and sale-related keyword matching for domain parking and sale, and others, and finally the validation from threat intelligence.

• **Chat Functionality Identification.** First, chat interaction is the most distinctive feature of ChatGPT. Our empirical analysis revealed that the chat function is primarily implemented via the <*textarea*> tag in HTML. Consequently, we identified chat-functional websites using a filter method anchored in the <*textarea*> tag. Furthermore, we used the term "chat" along with its synonyms like "dialogue" and its equivalents in multiple languages, including several non-English (like Chinese and Japanese), to match the content of the pages. Pages without chat-related keywords were excluded under the assumption that they lacked relevance to chat functionality. These websites are highly likely to be those that imitate ChatGPT, such as mirror sites, among others [82].

• **Underground Cybercrime Identification.** Then, through empirical analysis, we identified 2 typical categories of underground industries in ChatGPT-related squatting domains, namely, gambling and pornography. These two types of websites exhibit distinct text content features, consistent with the conclusions drawn from other underground industry research [93, 95]. Consequently, we designed a recognition method based on text content. After balancing the data obtained from the empirical analysis, we eventually selected 100 websites each from gambling, pornography, and other category as our training data. Before every processing (including labeling, training and predicting), we translated non-English web content to English with the interface of DeepL [22]. Subsequently, we train a multi-classifier based on the BERT model [23] to categorize the textual content of all website titles.

• **Domain Parking and Sale Identification.** Parking domains indicate that their owners are seeking profit through traffic monetization. Based on the Name Server (NS) records of the domains we acquired, we compare them with the NS records of popular domain parking services [46, 47, 88]. Besides, through empirical analysis, we discovered that some registrars offer domain name sale-help services. Domain owners can configure related display pages on these registrars (as example in Figure 8), so that when users access the domain (e.g., *chatgptcss.com*), they will receive the sale information of this domain, significantly enhancing the domain's exposure and aiding in its sale. For the sale display pages, we employ a set of keywords associated with domain sales based on our empirical study, such as "for sale", to classify.

• **Threat Intelligence Verification.** Beyond the three identification methods that we developed, we also leverage the analytic results of renowned threat intelligence as supplementary information. We supplement the malicious information for *each domain that has web content* by crawling the analytic

[3]https://pypi.org/project/python-whois/

[4]https://pypi.org/project/beautifulsoup4/

results from VirusTotal [36]. Furthermore, we collected 6 prominent open-source threat intelligence feeds, including URLHaus [85], BlackWeb [13], Stopforum Spam [77], Spamlist [78], Dyn Malware Feeds [24], and Zonefiles [98]. By contrasting these threat intelligence sources, we analyze whether any ChatGPT-related squatting domains with webpages are flagged as malicious.

### D. Evaluation

To evaluate the effectiveness of our identification method for ChatGPT-related domains and classification model, we employ a combination of random sampling and manual analysis. For a randomly sampled dataset of 100 domains, two researchers jointly annotate them, noting whether the domain genuinely relates to ChatGPT and the web page classification category. For inconsistent annotations, a third researcher is brought in for confirmation, ultimately resulting in a batch of high-quality annotated data. On the 100 annotated FQDNs, we find that our domain identification algorithm achieves 100% accuracy and 100% recall rate. Moreover, the accuracy of multi-classification is 93%, and the recall for gambling and porn is specifically 97% and 95%. Through manual analysis, we observe that the model's misclassifications predominantly occur in the "other" category, largely due to interference from little content on webpages to judge its usage. For instance, displaying only information irrelevant to inferring website purposes, such as website downtime or notices of website redesign and updates.

## IV. Characteristics of ChatGPT-Related Domains

In this section, we conduct the first comprehensive measurement and review of the ChatGPT-related squatting domains ecosystem. This analysis includes the examination of DNS traffic trends, domain registration distribution, infrastructure, web content and intent behind the registrations, along with the relevant security threat.

### A. Escalating Trend

PDNS records the DNS requests for ChatGPT-related domains and their responses, along with the time intervals when the domain was resolved. So, we can ascertain the *query volume* and *active periods* for ChatGPT-related domains [41, 48, 50]. Query volume means the total number of requests for a specific domain recorded in the PDNS dataset. Active period is the time interval between the first and last times the domain was resolved. As our collection comprises unofficially ChatGPT-related squatting domains, we also compare them with 3 official domains and their subdomains.

**Finding 1. From the DNS resolution standpoint, ChatGPT has led to a quick rise in ChatGPT-related squatting domains.** The red line in Figure 3 shows the total number of requests for ChatGPT-related squatting domains. Compared to when ChatGPT-3.5 was first released, the traffic has gone up 23.68 times by September 2023. We found a strong correlation between the visit trends of ChatGPT-related squatting domains

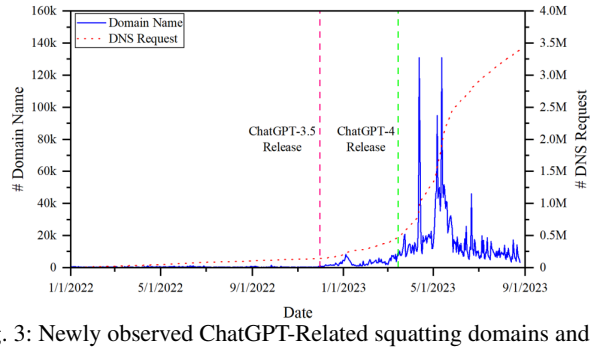


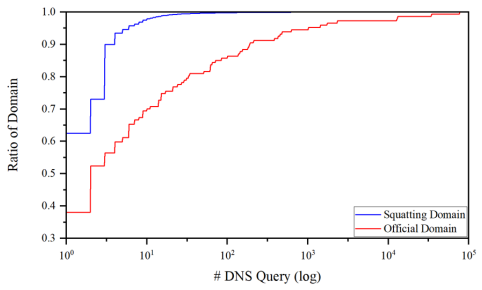
Fig. 3: Newly observed ChatGPT-Related squatting domains and their DNS resolutions.

and official sites, and the updates and major events of ChatGPT. SimilarWeb analyzed the global traffic (i.e., page views) of ChatGPT's website [76]. The page views of the official sites peaked in May, then the growth slowed and even showed a downward trend. We believe the surge in DNS traffic is linked to several updates by OpenAI [43], like changes in privacy, user data control, and the resumption of the Italian service. The later steady growth might be related to the release of user apps, as some of the traffic moved to mobile platforms. On the other hand, we noticed that even though the growth of the official ChatGPT website slowed down (or even declined) in May, the number of requests for ChatGPT-related squatting domains kept rising. As of September 2023, the growth rate continues to increase, showing that ChatGPT has a lasting effect on squatting domains. In addition, the blue line in Figure 3 shows the growth trend of newly observed domains. We noticed that the release of ChatGPT-3.5 led to a small increase in the number of domains (with almost a 9-fold growth seen in January 2023). However, the significant impact on squatting domains happened after the launch of GPT-4, with several increases in domain numbers.

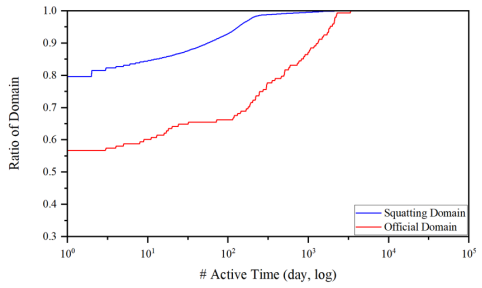
**Finding 2. ChatGPT-related squatting domains use ChatGPT keywords to effectively draw in user visits, with over 31k domains receiving more than 1,000 DNS requests.** Figure 4(a) shows that the query volume for ChatGPT-related squatting domains is generally less than official domains, with 97.45% of squatting domains getting fewer than 10 requests. However, we still found 291,892 domains that got more than 100 DNS requests, with a significant 31,226 domains exceeding 1,000 requests. Table II lists the top 10 squatting domains by query volume. Interestingly, we found that *chatgpt4youtube.com* is an unofficial Chrome plugin used for the real-time summary of video content, achieving 3,088 DNS requests. Also, we found an unofficial domain, *theb.ai*, that offers chat features similar to ChatGP with 214 subdomains, e.g., *chatgtp.theb.ai*. This domain not only got 2,906 DNS queries but also secured a domain rank of 58,983 (in the Top 100k). The chat features on this site include not only the official ChatGPT models but also their own. Notably, this unofficially operated website profits by offering services similar to the official ones, even attracting substantial user traffic. The active period of a domain can reflect its level

TABLE II: Query number of Top 10 ChatGPT-related squatting domains.

| FQDN | SLD | Category | # DNS Query (%) | Top 100k (SLD) |
|---|---|---|---|---|
| www.chatggpt.buzz | chatggpt.buzz | Other | 7,212 (0.16%) | Outside |
| chat.lai-ai.com.m.alikunlun.com | alikunlun.com | Other | 5,102 (0.15%) | 2,063 |
| chatcdn.ailiao360.com.w.kunluncan.com | kunluncan.com | Other | 4,880 (0.14%) | 1,917 |
| chat-ai.logcg.com | logcg.com | Chat-Function | 4,076 (0.12%) | Outside |
| openai-public.s3-us-west-2.amazonaws.com | amazonaws.com | Other | 3,831 (0.11%) | 2 |
| chat-gpt.org | chat-gpt.org | Chat-Function | 3,822 (0.11%) | Outside |
| ai-chatbot.s3.us-west-2.amazonaws.com | amazonaws.com | Other | 3,309 (0.09%) | 2 |
| chatcdn.ailiao520.com.w.kunluncan.com | kunluncan.com | Other | 3,095 (0.09%) | 1,917 |
| chatgpt4youtube.com | chatgpt4youtube.com | Chat-Function | 3,088 (0.09%) | Outside |
| chatbot.theb.ai | theb.ai | Chat-Function | 2,906 (0.08%) | 59,977 |




(a) ECDF of DNS query volume.




(b) ECDF of domain active period.

Fig. 4: Distribution of query volume and active period.

TABLE III: Keyword location of ChatGPT-related domains.

| - | Count | SLD-Chat (%) | | | SLD-nonChat (%) | | |
|---|---|---|---|---|---|---|---|
| **FQDN** | 1,357,638 | 708,963 (52.2%) | | | 648,675 (47.8%) | | |
| **SLD** | 119,907 | 59,084 (49.3%) | | | 60,823 (50.7%) | | |
| | | **<3.5** | **3.5~4** | **>4** | **<3.5** | **3.5~4** | **>4** |
| | | 16.6% | 47.1% | 36.3% | 76.6% | 12.9% | 10.5% |

* <3.5 means registered before the release of ChatGPT-3.5; 3.5~4 means registered between the release of ChatGPT-3.5 and GPT-4; >4 means registered after the release of GPT-4.

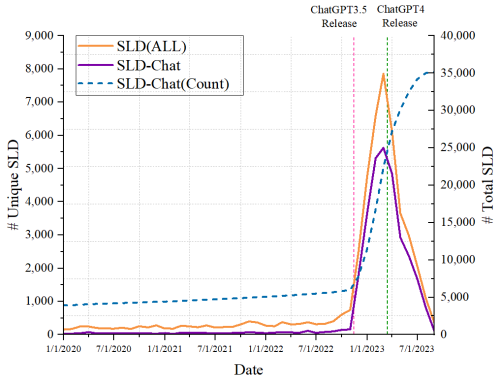



Fig. 5: Registration trend of ChatGPT-related domains.

of activity. As shown in Figure 4(b), despite a generally shorter active period compared to official domains, there still exist 9,507,539 ChatGPT-related squatting domains that have remained active for over 100 days, even 610,938 over 1,000 days. Upon analyzing squatting domains with active periods exceeding 1,000 days, we found that long-active domains did not exhibit any significant malicious behavior. For example, *openai.ru* is a domain registered in Russia in 2016. This website was constructed by volunteers interested in OpenAI's technology and has remained active since its establishment.

### *B. Domain Generation Trend*

Regarding the identified 119,907 SLDs, we are able to obtain their registration information based on the WHOIS records. Due to certain constraints, including query restrictions for country code top-level domains (ccTLDs) and privacy restrictions under the GDPR [52], we obtained valid registration information for 57.09% of all SLDs.

Based on the method of keyword embedding in domain generation, we categorized SLDs into two groups for analysis: those containing ChatGPT-related keywords in SLD (SLD-Chat) and those with keywords present in the subdomain instead (SLD-nonChat). The SLD-Chat group indicates that domains with ChatGPT-related keywords were generated through domain registration, while the SLD-nonChat group suggests that keywords were embedded through the configuration of subdomains, implying no relevance to registration. Table III displays the quantity distribution of two types of domains.

**Finding 3. Through analysis of registration dates of ChatGPT-related squatting domains, we discovered evidence of opportunistic bulk registration being undertaken by organized groups.** First, we discovered that the primary method of generating ChatGPT-related squatting domains involves directly registering SLDs that contain relevant keywords, accounting for 52.2% of such squatting domains. Figure 5 depicts the temporal distribution of ChatGPT-related

TABLE IV: Top 10 registries and registrars for FQDNs of SLD-Chats.

| TLD | # SLD | Registrar | # SLD |
|---|---|---|---|
| .com | 21,591 | GoDaddy | 7,051 |
| .cn | 2,284 | Alibaba Cloud Computing | 5,806 |
| .chat | 1,879 | NameCheap | 3,502 |
| .net | 1,505 | Squarespace Domains | 2,486 |
| .org | 998 | DNSPod | 1,527 |
| .xyz | 871 | MarkMonitor | 1,249 |
| .online | 856 | Dynadot | 1,141 |
| .com.cn | 454 | NameSilo | 748 |
| .ru | 443 | Gname.com Pte | 708 |
| .nl | 429 | Amazon Registrar | 516 |
| 445 TLDs | | 1,072 Registrars | |

squatting domain registrations. Looking at the overall trend, the popularity of ChatGPT-related events significantly stimulated the domain registration industry. It is noteworthy that opportunistic squatting cases began to emerge towards the end of 2022, influenced by the release of ChatGPT-3.5. This led to a surge in domain registrations, and 83.4% of SLD-Chat registered after ChatGPT-3.5. And the underground industry began to exploit the traffic of ChatGPT. For instance, *chatgpt-porn.pro* registered in February 2023, despite containing the keyword "chatgpt", is actually a pornographic website. Regrettably, due to the protection of registrant information by the GDPR, it is challenging for us to ascertain whether the peak in domain registrations observed in April 2023 was due to opportunistic bulk registrations. However, through an analysis of registration timing and registrar concentrations, we identified several cases that suggest bulk squatting. For instance, 16 domains registered with the Cloud Yuqu registrar, all occurring within a half-hour timeframe, appear to be generated from the term "chatgptplus" for domain squatting. Examples include *chatgptpplus.com* and *chatgpttplus.com*. Moreover, we discovered that opportunistic domain intermediaries are promoting the sale of AI-related domains, particularly those associated with ChatGPT, such as *buyaidomains.com*.

**Finding 4. Until now, we found few domain registrars that are aware of the potential risks associated with ChatGPT-related squatting domains, nor have any measures been taken.** By analyzing the registries and registrars, we attempt to infer the registration choices for SLD-Chats. And we found that ChatGPT-related squatting SLDs collectively cover 445 TLDs and 1,072 registrars. Table IV shows the top 10 registries and registrars according to the domain registration volume. Interestingly, 16 of these TLDs incorporate keywords related to ChatGPT, for example, "ai" and "chat" are not only TLDs but also two keywords strongly associated with ChatGPT. Regrettably, through the examination of registry and registrar results, we found that there are virtually few registration vendors recognizing the potential security risks of ChatGPT-related squatting domains at present, without implementing any measurements. This lack of regulation provides substantial opportunities for exploitation by cybercriminals.

**Finding 5. Beyond opportunistic registrations, configuring subdomains, a more economical method, may cause levelsquatting threat.** We observed that 47.8% of squatting FQDNs were generated via subdomain configuration, indicating that SLD-nonChat is also a popular method of squatting domain creation. We hypothesize that this trend may be due to the relative ease and cost-efficiency associated with subdomain configuration, as it eliminates the need for new domain registration fees. Within SLD-nonChat, some subdomains are configured under user-maintained apex domains. ChatGPT has also exerted a significant influence on the domain names associated with the underground industry. For instance, we identified *lashou365.com* as an underground gambling website based on historical records [39]. In the wake of the widespread discussions sparked by ChatGPT, this domain owner configured a total of 236 related subdomains for eye-catching.

Additionally, the trend of using third-party network services to create ChatGPT-related domains is prevalent, including using Content Delivery Network (CDN) services with 1,359 FQDNs set up under *cloudflare.net* [17], and cloud storage with 19,890 FQDNs set up under *amazonaws.com* [4]. However, these domains are often exceptionally long and can be utilized for levelsquatting scams. For example, the official domain is embedded into the subdomain of *chatgpt.com.admin-eu2.cas.ms* This would mislead mobile users who could not see the entire domain due to display space limitations, making them vulnerable to phishing scams.

Furthermore, these inexpensive or even free third-party services are particularly prone to misuse by adversaries, such as the legitimate AI model-sharing platform of Hugging Face [38], *hf.space*. Based on the SLD (*hf.space*) coupled with manual analysis, we conclusively identified 5,375 pertinent domains. Upon manual verification, we found that some users leverage Hugging Face to establish their own intelligent dialogue services, such as *jaehwi000-chatgpt4.hf.space*. However, these established services are not officially owned and may present security risks, such as the theft of user tokens, as described in Section IV-D.

**Finding 6. Various squatting techniques are adopted to create ChatGPT-related squatting domains, demonstrating a great misuse potential.** Table V presents the keyword selection distribution among all identified domains, categorized into 3 types: seed keywords, squatting keywords, and combined keywords. Regrettably, we discovered various squatting techniques within ChatGPT-related domains. For instance, combosquatting [41], denoted as "combined keywords" in Table V, involves combining several keywords to create squatting domains. Besides, some keywords subjected to squatting transformations frequently appear in domain names, which as more malicious with deceptive phishing attributes. For example, *chaudeechatte.mypornchat.com* is an underground pornographic site embedded with the keyword "claude" to borrow its popularity for fraud.

### C. Infrastructure

Given that the domain names and their resolution results extracted from the PDNS dataset include historical data,

TABLE V: Keywords distribution of ChatGPT-related squatting domains.

| Seed Keywords | | | Combined Keywords | | | Squatting Keywords | | |
|---|---|---|---|---|---|---|---|---|
| **Keyword** | **# FQDN (%)** | **# Top 100k (%)** | **Keyword** | **# FQDN (%)** | **# Top 100k (%)** | **Keyword** | **# FQDN (%)** | **# Top 100k (%)** |
| ai | 861,112 (63.43%) | 517,913 (83.99%) | chat+gpt | 432,618 (31.87%) | 77,867 (12.63%) | cloude | 27,560 (2.03%) | 1,506 (0.24%) |
| chat | 700,799 (51.62%) | 131,715 (21.36%) | open+ai | 409,046 (30.13%) | 347,981 (56.43%) | hatbot | 11,253 (0.83%) | 5,557 (0.90%) |
| gpt | 625,284 (46.06%) | 196,362 (31.85%) | ai+chat | 202,357 (14.91%) | 31,214 (5.06%) | gpot | 10,640 (0.78%) | 2,034 (0.33%) |
| open | 432,627 (31.87%) | 363,056 (58.88%) | ai+gpt | 176,863 (13.03%) | 112,031 (18.17%) | gpmt | 9,549 (0.70%) | 1,688 (0.27%) |
| claude | 12,733 (0.94%) | 691 (0.11%) | chat+open | 20,803 (1.53%) | 13,638 (2.21%) | gppt | 8,995 (0.66%) | 7,207 (1.17%) |
| copilot | 2,849 (0.21%) | 286 (0.05%) | ai+cloude | 17,939 (1.32%) | 721 (0.12%) | gmpt | 4,374 (0.32%) | 2,338 (0.38%) |

* "Top100k" means the number of domain names whose SLD are ranked in Top 100,000.

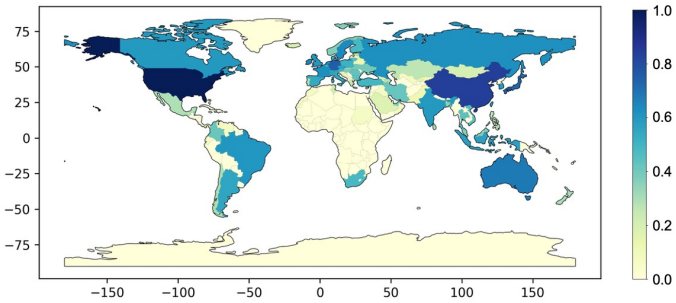


Fig. 6: Geographical IP distribution of ChatGPT-related squatting domains.

TABLE VI: Top 10 countries or regions and ASNs for ChatGPT-related squatting domains.

| Country or region | # FQDN | ASN | # FQDN |
|---|---|---|---|
| USA | 217,464 | 8075 (Microsoft) | 152,991 |
| CHN | 10,794 | 16509 (Amazon-02) | 40,928 |
| SGP | 6,219 | 14618 (Amazon-AES) | 24,712 |
| JPN | 3,524 | 396982 (Google-Cloud) | 10,968 |
| SWE | 1,351 | 13335 (Cloudflare) | 6,016 |
| NLD | 1,236 | 32934 (Facebook) | 2,767 |
| CZE | 1,187 | 15169 (Google) | 2,741 |
| FRA | 1,023 | 13414 (Twitter) | 1,907 |
| DEU | 990 | 20940 (Akamai) | 1,765 |
| IRL | 839 | 19679 (Dropbox) | 1,642 |
| **92 Countries or regions** | | **1,865 ASNs** | |

we ascertain their current state by actively performing DNS resolution for several important query types, including *A*, and *NS*. We present the results of our active queries in Table VII. As of November 2023, we observe that 67.6% of the FQDNs can still be resolved through DNS.

**Finding 7. ChatGPT-related squatting domains rely on a handful of web hosting operators, which offer valuable opportunities to combat and mitigate ChatGPT-related abuse risks.** Through query for *A* record, we could obtain the IP address to which the domain resolves, as well as the associated host information. We employed MaxMind [54] to acquire geographic information on the IP addresses from the resolution results, which are illustrated in Figure 6. We observed that the resolution results of these domains are distributed across 92 countries or regions, encompassing 1,865 Autonomous System Numbers (ASNs). The overall distribution of their infrastructure exhibits long-tail characteristics, where leading providers constitute a substantial proportion, as shown in Table VI. Geographically, the United States holds a significantly dominant share, accounting for 16.02% of FQDNs. The number of domains it covers exceeds that of the second-largest contributor, China, by a factor of over 20.

Further, in conjunction with existing work [49], we constructed a list of third-party cloud operators, comprising nine renowned companies [5]. By matching the AS information in the IP addresses, we identified domains hosted on third-party cloud services. As inferred from the top 10 ASNs in Table VI, third-party web hosting services appear to be predominantly preferred by domain owners. This is evidenced by the fact that 278,169 (20.5%) of FQDNs are hosted under such famous cloud services, based on the cloud-related keywords. We observed that akin to market share rankings [14], renowned hosting vendors, such as Microsoft Azure [56], Amazon [5] and Google Cloud [32], are the preferred choices for ChatGPT-related squatting domains. Furthermore, we unearthed a container hosting platform, Dropbox [26], covering 1,642 FQDNs. For example, *chatgpt-web-production-d086.up.railway.app* is a project created via *railway.app*[6] and hosted on Dropbox.

Based on our findings, we contend that current third-party web hosting services have become a breeding ground for abusers. From another perspective, we believe that these web hosting vendors are crucial in combating the abuse of ChatGPT-related squatting domains. The risk can be effectively mitigated by inspecting the content of hosted pages.

[5]This list includes "aws", "google", "cloudflare", "ali", "linode", "digitocean", "tencent", "azure", "akamai".

[6]Railway App is an instant deployment platform

TABLE VII: Active DNS resolution and HTTP responses.

| - | # FQDN(%) | # SLD(%) | Top 100k |
|---|---|---|---|
| **Active DNS** | 917,513 (67.6%) | 74,406(62.1%) | 2,734 |
| **Active HTTP** | 123,333 (9.1%) | 35,073(29.3%) | 935 |
| **HTTP Content** | 71,379 (5.3%) | 18,867(15.7%) | 814 |

* "Top100k" means the number of domain names whose SLD are ranked in Top 100,000.

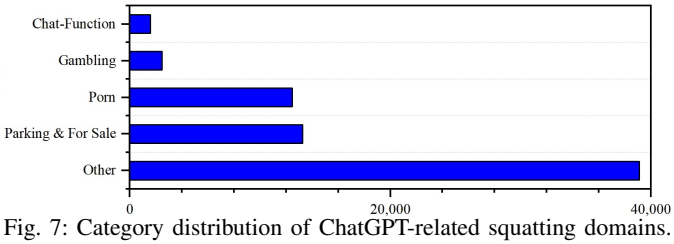


Fig. 7: Category distribution of ChatGPT-related squatting domains.

### D. Web Content and Intent

To identify the web content of ChatGPT-related squatting domains, we crawled their HTTP responses and webpages. According to Table VII, merely 9.1% of the domains continue to provide HTTP services, i.e., they return HTTP status codes *1xx*, *2xx* and *3xx*. Furthermore, we analyzed the web content and the intent of these squatting domains, as depicted in Figure 7. Although the registration of unofficial squatting domains is no longer a benign act (not proactive registration from the official ChatGPT for protective purposes), distressingly, we actually detected a considerable amount of abuse in these domains.

**Finding 8. Judging by the intent of their webpages, ChatGPT-related squatting domains remain in their "nascent" stage, with only 5.3% having configured page content.** We initially conducted a preliminary content analysis of the 123,333 websites still offering HTTP services. First, we filtered out certain pages with little substantive content, including those with excessively brief content (less than 10 characters), those comprising solely of web configuration pages (such as Apache, Nginx, etc.), and a series of "page not found" prompts. Subsequently, we found that despite the substantial quantity of ChatGPT-related squatting domains, only 5.3% offered valid pages. This suggests that the majority of these domains are registered opportunisticly, targeting the trending topic of ChatGPT, without the configuration of significant page content. Furthermore, through analyzing NS records and comparing these with NS lists of domain parking services identified in previous studies [46, 88], we discovered that 7,583 ChatGPT-related squatting domains are in the state of domain parking. These originate from 8 different domain parking vendors. We speculate that these parked domains were initially registered opportunistically and subsequently capitalized upon through traffic monetization to derive profits. In addition, we identified another speculative profit-seeking approach: the use of the registrar's domain display pages to attempt the resale of owned domains related to ChatGPT [3]. Figure 8 depicts a display page for *chatgptcss.com* that is being offered for sale. This page displays relevant information about its registrant and provides a purchase link for interested buyers. We identified 5,666 domains being offered for sale, indicating that these registrants, following the popularity of ChatGPT, registered domains and subsequently hoped to sell them at a higher price for profit.

**Finding 9. After digging into their web content, we discovered that the significant traffic instigated by ChatGPT has also become a conduit for luring users to**

Fig. 8: Example of a domain name for sale.

**gambling or pornographic activities.** Based on the machine learning model trained on webpage titles and content (Section III-C), we discovered that among ChatGPT-related squatting domains with valid page contents, 12,475 (17.48%) are related to adult content and 2,460 (3.45%) are associated with illegal gambling content. The creation methods of these domains related to traditional underground industries are relatively uniform. They all opt for configuring sub-domains, a method that avoids the cost of new domain registration. Specifically, they configure subdomains on apex domains, embedding ChatGPT-related keywords. For instance, the domain *automan520.com* has configured 7,546 subdomains, like *chatgpt987814.automan520.com*. We speculate that there are two primary reasons why these underground industries embed ChatGPT-related keywords. On one hand, leveraging the popularity of ChatGPT may increase the visibility of these illicit websites to users, such as enhancing their ranking in search engines [10]. On the other hand, by configuring long sub-domains and constructing levelsquatting abuses, they can deceive users into clicking on these links. In fact, we found that the overall request volume for *automan520.com* and its subdomains totaled 7,725, suggesting that the use of ChatGPT-related keywords indeed had a certain promotional effect.

**Finding 10. Beyond traditional underground activities, the use of ChatGPT has led to a new security issue: the creation of unauthorized mirror websites of ChatGPT.** By analyzing the *<textarea>* filed with chat-related keyword filtering, we identified that 1,571 domains have implemented features or services analogous to the intelligent conversation capabilities of ChatGPT on their webpages. Given the high interactivity inherent in the analysis of dialogue features,

which resists complete automation, our examination of such websites was limited to manual analysis of these websites with chat functions. Notably, while OpenAI considerably endorses the development of applications predicated on ChatGPT, it categorically forbids the monetization of its services, such as selling, leasing, or distributing them [67]. In spite of these prohibitions, we observed mirror websites hosted on ChatGPT-related squatting domains purporting to offer question-and-answer services based on the official ChatGPT model for profit. As depicted in Figure 9, once the allocated quota of free usage is exhausted, payment is required for continued access to the service. In this work, we define squatting domains embedding ChatGPT-related keywords, designed to deceive users into perceiving their chat services as officially ChatGPT for profit, as unauthorized mirror websites. However, these websites are not officially sanctioned by OpenAI to provide commercial services and thus contravene OpenAI's official regulations [67].

Interestingly, our findings indicate that the majority of these unauthorized dialogue service provisions are concentrated in China. This could potentially be attributed to the usage restrictions imposed by OpenAI on Chinese users [66] and the censorship from Chinese GFW [83]. The escalating demand for ChatGPT among users who experience difficulties with its official functionalities has resulted in a surge of unauthorized services. Concurrently, it has also catalyzed the emergence of an industry, characterized by the provision of templates and even website construction tools for setting up services analogous to ChatGPT. For instance, a website construction template originating from Github [7] has facilitated the establishment of at least 47 websites offering similar dialogue functionalities. This website even has promotional activities such as offering free chat opportunities in exchange for inviting friends. Additionally, we found that the establishment of unauthorized dialogue websites based on ChatGPT is emerging in other countries, including those without usage restrictions, such as Japan (*chatgptjapan.org* with 8 requests within 22 active days) and Germany (*chatopenai.de* with 8 requests). Regrettably, through combined analysis with TI, we discovered some mirror sites exploiting ChatGPT's popularity to entice users into propagating their malicious software. For instance, *chatgpt.shrwei3.top* (with 64 requests within 78 active days) lures users into downloading malware through prompts to download its client.

More seriously, we identified mirror sites bearing a striking resemblance to the official ChatGPT website, with the same icon and webpage content. We conjecture that these could potentially be phishing sites maliciously deployed by attackers, as illustrated in Figure 1 (in Section I). Drawing on existing work that detects phishing sites based on webpage similarity [1, 45], we evaluated brand resemblance by determining the presence of official brand images on websites offering chat functionalities. Specifically, we convert all images to grayscale for evaluation, and scale the official brand images to various

[7]https://github.com/dirk1983/chatgpt

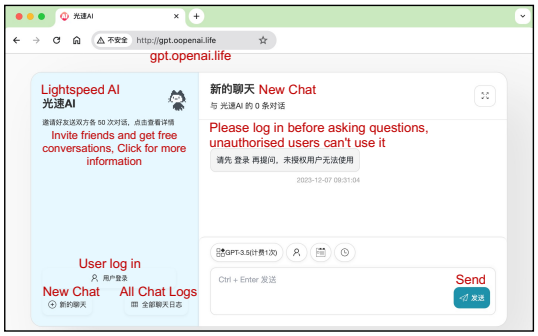



Fig. 9: Example of an unauthorized mirror ChatGPT website with payment requirements.

proportions for pixel matching within the pages. Ultimately, we identified 33 webpages exhibiting the appearance of the official brand, indicative of phishing intentions and trademark infringement threats.

**Finding 11. The threat intelligence significantly trails behind in its ability to detect these abuse activities of ChatGPT-related squatting domains.** To evaluate the impact of these abuses, we utilized 6 public threat intelligence (mentioned in Section III-C) and renowned VirusTotal [36]. Due to request limitations, we only fetched threat intelligence of 71,954 (5.3%) domains that configured webpages. The results revealed that only 3,157 (4.4%) domains were marked by VirusTotal as malicious. Furthermore, we discovered that only 3,792 domains were marked as malicious by public threat intelligence, all flagged by BlackWeb, with two domains also marked by Stopforum Spam. However, public threat intelligence lacks definitive information on the nature of the threats. By cross-validating threat intelligence, we contend that the current understanding within the security community of the threats introduced by ChatGPT is severely lagging. Particularly, there is a significant deficiency in the understanding of novel security threats related to ChatGPT-associated squatting domains.

## V. Discussion

**Limitations.** Despite our best efforts, there are still some limitations to be considered. First, our PDNS dataset may exhibit geographical distribution bias. However, given the massive volume of DNS data, we believe our domain data can still reflect the ecosystem of ChatGPT-related domains comprehensively. Second, the categories are identified through manual analysis with a limited labeled dataset, and may not be exhaustive. Nevertheless, by cross-validating using external threat intelligence data and searching for security risks related to ChatGPT, we believe that the risks we have disclosed are among the most noteworthy and impactful within the context of ChatGPT-related threats.

**Lessons Learned.** Despite the numerous abuse risks we identified in ChatGPT-related squatting domains, as of now, few registries, registrars, and even third-party hosting platforms have implemented protective measures against such

malicious squatting activities, thereby fostering an environment conducive to misuse. Therefore, based on our findings, we propose the following recommendations to the security community, with the aim of alleviating the misuse of ChatGPT-related squatting domains. First, we recommend that registrars and registries can recognize the potential security risks of ChatGPT-related squatting domains, and take appropriate protective measures. For instance, verify the registrant origin of squatting domains and restrict unofficial bulk malicious registrations. Second, we recommend that third-party hosting services rigorously review hosted content to avoid the deployment of abusive activities, for example, illicit gambling and porn content. Last but not least, we recommend that official websites (including ChatGPT, Claude, and so on) take this matter seriously and consider proactive registration for protection. We also open-source part of identified ChatGPT-related squatting domains and their misuse behaviors, thereby offering a valuable resource for comprehensive analysis by the entire security community.

**Ethics Considerations.** Our entire experimental process strictly adhered to established ethical guidelines, notably the Belmont Report [30] and the Menlo Report [40]. For data collection, we confined our scope to domain names and their resolution results and counts, without involving any user-end information. Therefore, we believe there are minimal ethical risks in our data collection and analysis process. Furthermore, our analysis results of ChatGPT-related squatting domains offer enduring benefits for the cybersecurity community.

## VI. Related Work

**Domain Abuse.** Squatting attack is one of the most common forms of domain abuse [19, 31, 33, 84]. It involves the creation of domains closely resembling target domains, designed to phish users into clicking or visiting and hijack their web traffic, potentially leading to the disclosure of personal privacy data, such as passwords. The introduction of Internationalized Domain Name (IDN) has significantly expanded the domain name space, but it has also brought about homograph attack techniques [37, 50, 72, 80]. In addition to homograph attacks, a variety of squatting attack techniques have evolved, such as typosquatting (mistyping of popular authoritative domains) [2, 20, 81, 87], bitsquatting (random bit-flipping in domains) [63], soundsquatting (abusing the sound similarity of words in domains) [62], combosquatting (utilizing word concatenation to form related words) [41], and levelsquatting (abusing the display limitations of long subdomains) [27].

Moreover, domain names, as the initial link in accessing the network, i.e., obtaining the corresponding host IP address, are frequently abused in a variety of cybercriminal activities. In particular, they are used for malicious promotion, such as BlackHat Search Engine Optimization (SEO) techniques [28, 94], malware propagation, such as DGA domains for botnet [7, 69, 91], and fraudulent and phishing activities [51, 86].

**Abused Domain Detection.** Considerable efforts have been dedicated by both academia and industry to develop effective detection methods for malicious domains that are subject to misuse. The most predominant approach involves detection based on DNS resolution traffic [96], which includes methods that detect based on the malicious association of IP addresses and domain names [8, 79], detect changes in resolution traffic [9, 12], and detect abnormal registration behaviors [34]. In addition, there are detection methods based on page content, such as phishing domain detection based on the similarity of page content [51, 53, 89, 97].

**ChatGPT-related Cybercrime.** Several studies have also highlighted the misuse of ChatGPT in cybercriminal activities and other malicious behaviors. Nils' work [11] revealed that ChatGPT has been utilized by criminals for online phishing, and some studies further analyzed the impact of ChatGPT on phishing attacks, finding that phishing activities incorporating ChatGPT have a higher success rate of deceit [75, 92]. Filipo's study [74] analyzed the erroneous information output by ChatGPT on social platforms, which can misguide users.

In conclusion, our work is the first to identify ChatGPT-related squatting domains from the comprehensive perspective of DNS resolution, followed by a thorough and systematic analysis, and we reveal previously unknown new abusive behaviors related to ChatGPT. We believe that our findings hold considerable value for understanding ChatGPT-related misuse and even cybercriminal activities.

## VII. Conclusion

The popularity of ChatGPT brings significant abuse threats of ChatGPT-related squatting domains, an issue that is growing rapidly yet remains inadequately addressed by the security community. We developed an efficient approach to identify ChatGPT-related squatting domains from an extensive PDNS dataset. In the end, we identified over 1.3 million ChatGPT-related squatting domains, including SLD-Chat directly registered from registrars and those obtained by configuring subdomains. By examining identified ChatGPT-related squatting domains, we conducted the first comprehensive measurement study of this ecosystem. With a 5.3% active website rate, these domains pose considerable threats, including the promotion of illegal underground activities and novel forms of fraud with chat functions. Despite these findings, key stakeholders like domain registrars, web hosting providers and existing threat intelligence seem oblivious to these risks, showing few signs of implementing protective measures. We hope our work, which unveils this abuse ecosystem, prompts an increased focus on this issue and the deployment of robust protective measures against ChatGPT-related squatting domain abuse.

## Acknowledgment

We thank all the anonymous reviewers for their valuable comments to improve this paper. This research is supported by the National Natural Science Foundation of China (62102218, U19B2034), CCF-Tencent Rhino-Bird Young Faculty Open Research Fund (CCF-Tencent RAGR20230116). Haixin Duan is supported by the Taishan Scholars Program.

## REFERENCES


[1] S. Abdelnabi, K. Krombholz, and M. Fritz. Visualphishnet: Zero-day phishing website detection by visual similarity. In J. Ligatti, X. Ou, J. Katz, and G. Vigna, editors, *CCS '20: 2020 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, USA, November 9-13, 2020*, pages 1681–1698. ACM, 2020.

[2] P. Agten, W. Joosen, F. Piessens, and N. Nikiforakis. Seven months' worth of mistakes: A longitudinal study of typosquatting abuse. In *22nd Annual Network and Distributed System Security Symposium, NDSS 2015, San Diego, California, USA, February 8-11, 2015*. The Internet Society, 2015.

[3] Ali Cloud. Domain for sale display page. https://help.aliyun.com/zh/dws/user-guide/domain-name-display-page, 2024.

[4] Amazon. Amazon AWS. https://aws.amazon.com.

[5] Amazon. Amazon Cloud. https://aws.amazon.com/, 2023.

[6] Anthropic PBC. Claude. https://claude.ai/, 2023.

[7] M. Antonakakis, T. April, M. D. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou. Understanding the mirai botnet. In E. Kirda and T. Ristenpart, editors, *26th USENIX Security Symposium, USENIX Security 2017, Vancouver, BC, Canada, August 16-18, 2017*, pages 1093–1110. USENIX Association, 2017.

[8] M. Antonakakis, R. Perdisci, D. Dagon, W. Lee, and N. Feamster. Building a dynamic reputation system for DNS. In *19th USENIX Security Symposium, Washington, DC, USA, August 11-13, 2010, Proceedings*, pages 273–290. USENIX Association, 2010.

[9] M. Antonakakis, R. Perdisci, W. Lee, N. Vasiloglou, and D. Dagon. Detecting malware domains at the upper DNS hierarchy. In *20th USENIX Security Symposium, San Francisco, CA, USA, August 8-12, 2011, Proceedings*. USENIX Association, 2011.

[10] Backlinko Team. ChatGPT for SEO: Ultimate Guide, Tips & Prompts. https://backlinko.com/chatgpt-for-seo, 2023.

[11] N. Begou, J. Vinoy, A. Duda, and M. Korczynski. Exploring the dark side of AI: advanced phishing attack design and deployment using chatgpt. In *IEEE Conference on Communications and Network Security, CNS 2023, Orlando, FL, USA, October 2-5, 2023*, pages 1–6. IEEE, 2023.

[12] L. Bilge, E. Kirda, C. Kruegel, and M. Balduzzi. EXPOSURE: finding malicious domains using passive DNS analysis. In *Proceedings of the Network and Distributed System Security Symposium, NDSS 2011, San Diego, California, USA, 6th February - 9th February 2011*. The Internet Society, 2011.

[13] BlackWeb. Blackweb. https://github.com/maravento/blackweb/, 2023.

[14] BuiltWith. Web Hosting Usage Distribution on the Entire Internet. https://trends.builtwith.com/hosting/traffic/Entire-Internet, 2023.

[15] CBNData. Live ChatGPT on Douyin, producing huge traffic for profit? https://www.cbndata.com/information/267654, 2023.

[16] Christopher Boyd. Bogus Chat GPT extension takes over Facebook accounts . https://www.malwarebytes.com/blog/news/2023/03/bogus-chat-gpt-extension-takes-over-facebook-accounts, 2023.

[17] Cloudflare, Inc. Cloudflare. https://cloudflare.net/, 2023.

[18] A. Costello. Punycode: A bootstring encoding of unicode for internationalized domain names in applications (idna). Technical report, RFC 3492, March, 2003.

[19] S. E. Coull, A. M. White, T. Yen, F. Monrose, and M. K. Reiter. Understanding domain registration abuses. In K. Rannenberg, V. Varadharajan, and C. Weber, editors, *Security and Privacy - Silver Linings in the Cloud - 25th IFIP TC-11 International Information Security Conference, SEC 2010, Held as Part of WCC 2010, Brisbane, Australia, September 20-23, 2010. Proceedings*, volume 330 of *IFIP Advances in Information and Communication Technology*, pages 68–79. Springer, 2010.

[20] T. Dam, L. D. Klausner, and S. Schrittwieser. Typosquatting for fun and profit: Cross-country analysis of pop-up scam. *J. Cyber Secur. Mobil.*, 9(2):265–300, 2020.

[21] David Gewirtz. How to use ChatGPT to write code. https://www.zdnet.com/article/how-to-use-chatgpt-to-write-code/, 2023.

[22] DeepL. DeepL. https://www.deepl.com/translator, 2023.

[23] J. Devlin, M. Chang, K. Lee, and K. Toutanova. BERT: pre-training of deep bidirectional transformers for language understanding. In J. Burstein, C. Doran, and T. Solorio, editors, *Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, NAACL-HLT 2019, Minneapolis, MN, USA, June 2-7, 2019, Volume 1 (Long and Short Papers)*, pages 4171–4186. Association for Computational Linguistics, 2019.

[24] D. DNS. Dyn dns. http://security-research.dyndns.org/pub/malware-feeds/, 2023.

[25] DNSTwist. DNSTwist. https://github.com/elceef/dnstwist, 2023.

[26] Dropbox. Dropbox Storage. https://www.dropbox.com/, 2023.

[27] K. Du, H. Yang, Z. Li, H. Duan, S. Hao, B. Liu, Y. Ye, M. Liu, X. Su, G. Liu, Z. Geng, Z. Zhang, and J. Liang. Tl;dr hazard: A comprehensive study of levelsquatting scams. In S. Chen, K. R. Choo, X. Fu, W. Lou, and A. Mohaisen, editors, *Security and Privacy in Communication Networks - 15th EAI International Conference, SecureComm 2019, Orlando, FL, USA, October 23-25, 2019, Proceedings, Part II*, volume 305 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pages 3–25. Springer, 2019.

[28] K. Du, H. Yang, Z. Li, H. Duan, and K. Zhang. The ever-changing labyrinth: A large-scale analysis of wildcard DNS powered blackhat SEO. In T. Holz and S. Savage, editors, *25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, August 10-12, 2016*, pages 245–262. USENIX Association, 2016.

[29] P. V. Falade. Decoding the threat landscape: Chatgpt, fraudgpt, and wormgpt in social engineering attacks. *arXiv preprint arXiv:2310.05595*, 2023.

[30] U. S. N. C. for the Protection of Human Subjects of Biomedical and B. Research. *The Belmont report: ethical principles and guidelines for the protection of human subjects of research*. Department of Health, Education and Welfare, 1979.

[31] J. Golinveaux. What's in a domain name: Is cybersquatting trademark dilution. *USFL Rev.*, 33:641, 1998.

[32] Google. Google Cloud. https://cloud.google.com/, 2023.

[33] T. Halvorson, K. Levchenko, S. Savage, and G. M. Voelker. Xxxtortion?: inferring registration intent in the .xxx TLD. In C. Chung, A. Z. Broder, K. Shim, and T. Suel, editors, *23rd International World Wide Web Conference, WWW '14, Seoul, Republic of Korea, April 7-11, 2014*, pages 901–912. ACM, 2014.

[34] S. Hao, A. Kantchelian, B. Miller, V. Paxson, and N. Feamster. PREDATOR: proactive recognition and elimination of domain abuse at time-of-registration. In E. R. Weippl, S. Katzenbeisser, C. Kruegel, A. C. Myers, and S. Halevi, editors, *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016*, pages 1568–1579. ACM, 2016.

[35] X. He, S. Zannettou, Y. Shen, and Y. Zhang. You only prompt once: On the capabilities of prompt learning on large language models to tackle toxic content. *CoRR*, abs/2308.05596, 2023.

[36] Hispasec Sistemas Company. Virus Total. https://www.virustotal.com/gui/home/search. (Access in October, 2021).

[37] T. Holgers, D. E. Watson, and S. D. Gribble. Cutting through the confusion: A measurement study of homograph attacks. In A. Adya and E. M. Nahum, editors, *Proceedings of the 2006 USENIX Annual Technical Conference, Boston, MA, USA, May 30 - June 3, 2006*, pages 261–266. USENIX, 2006.

[38] Hugging Face. Hugging Face. https://huggingface.co/spaces, 2023.

[39] Internet Archive. Wayback Machin. https://web.archive.or, 2023.

[40] E. Kenneally and D. Dittrich. The menlo report: Ethical principles guiding information and communication technology research. *Available at SSRN 2445102*, 2012.

[41] P. Kintis, N. Miramirkhani, C. Lever, Y. Chen, R. R. Gómez, N. Pitropakis, N. Nikiforakis, and M. Antonakakis. Hiding in plain sight: A longitudinal study of combosquatting abuse. In B. Thuraisingham, D. Evans, T. Malkin, and D. Xu, editors, *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017*, pages 569–586. ACM, 2017.

[42] T. Koide, N. Fukushi, H. Nakano, and D. Chiba. Phishreplicant: A language model-based approach to detect generated squatting domain names. *CoRR*, abs/2310.11763, 2023.

[43] Kristi Hines. History Of ChatGPT: A Timeline Of The Meteoric Rise Of Generative AI Chatbots. https://www.searchenginejournal.com/history-of-chatgpt-timeline/488370/, 2023.

[44] Le Tiantian. Pinyin2hanzi. https://github.com/letiantian/Pinyin2Hanzi, 2015.

[45] Y. Lin, R. Liu, D. M. Divakaran, J. Y. Ng, Q. Z. Chan, Y. Lu, Y. Si, F. Zhang, and J. S. Dong. Phishpedia: A hybrid deep learning based approach to visually identify phishing webpages. In M. D.

Bailey and R. Greenstadt, editors, *30th USENIX Security Symposium, USENIX Security 2021, August 11-13, 2021*, pages 3793–3810. USENIX Association, 2021.

[46] B. Liu, Z. Li, P. Zong, C. Lu, H. Duan, Y. Liu, S. A. Alrwais, X. Wang, S. Hao, Y. Jia, Y. Zhang, K. Chen, and Z. Zhang. Traffickstop: Detecting and measuring illicit traffic monetization through large-scale DNS analysis. In *IEEE European Symposium on Security and Privacy, EuroS&P 2019, Stockholm, Sweden, June 17-19, 2019*, pages 560–575. IEEE, 2019.

[47] B. Liu, C. Lu, H. Duan, Y. Liu, Z. Li, S. Hao, and M. Yang. Who is answering my queries: Understanding and characterizing interception of the DNS resolution path. In W. Enck and A. P. Felt, editors, *27th USENIX Security Symposium, USENIX Security 2018, Baltimore, MD, USA, August 15-17, 2018*, pages 1113–1128. USENIX Association, 2018.

[48] B. Liu, C. Lu, Z. Li, Y. Liu, H. Duan, S. Hao, and Z. Zhang. A reexamination of internationalized domain names: The good, the bad and the ugly. In *48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2018, Luxembourg City, Luxembourg, June 25-28, 2018*, pages 654–665. IEEE Computer Society, 2018.

[49] D. Liu, S. Hao, and H. Wang. All your DNS records point to us: Understanding the security threats of dangling DNS records. In E. R. Weippl, S. Katzenbeisser, C. Kruegel, A. C. Myers, and S. Halevi, editors, *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016*, pages 1414–1425. ACM, 2016.

[50] M. Liu, Y. Zhang, B. Liu, and H. Duan. Exploring the characteristics and security risks of emerging emoji domain names. In V. Atluri, R. D. Pietro, C. D. Jensen, and W. Meng, editors, *Computer Security - ESORICS 2022 - 27th European Symposium on Research in Computer Security, Copenhagen, Denmark, September 26-30, 2022, Proceedings, Part III*, volume 13556 of *Lecture Notes in Computer Science*, pages 186–206. Springer, 2022.

[51] R. Liu, Y. Lin, X. Yang, S. H. Ng, D. M. Divakaran, and J. S. Dong. Inferring phishing intention via webpage appearance and dynamics: A deep vision based approach. In K. R. B. Butler and K. Thomas, editors, *31st USENIX Security Symposium, USENIX Security 2022, Boston, MA, USA, August 10-12, 2022*, pages 1633–1650. USENIX Association, 2022.

[52] C. Lu, B. Liu, Y. Zhang, Z. Li, F. Zhang, H. Duan, Y. Liu, J. Q. Chen, J. Liang, Z. Zhang, S. Hao, and M. Yang. From WHOIS to WHOWAS: A large-scale measurement study of domain registration privacy under the GDPR. In *28th Annual Network and Distributed System Security Symposium, NDSS 2021, virtually, February 21-25, 2021*. The Internet Society, 2021.

[53] S. Marchal, J. François, R. State, and T. Engel. Proactive discovery of phishing related domain names. In D. Balzarotti, S. J. Stolfo, and M. Cova, editors, *Research in Attacks, Intrusions, and Defenses - 15th International Symposium, RAID 2012, Amsterdam, The Netherlands, September 12-14, 2012. Proceedings*, volume 7462 of *Lecture Notes in Computer Science*, pages 190–209. Springer, 2012.

[54] MaxMind. IP Geolocation and Online Fraud Prevention. https://www.maxmind.com/en/home., 2023.

[55] MEGAN CERULLO. Criminals are using AI tools like ChatGPT to con shoppers. Here's how to spot scams. https://www.cbsnews.com/news/black-friday-shopping-scams-how-to-spot/, 2023.

[56] Microsoft. Azure. https://azure.microsoft.com/en-us, 2023.

[57] Microsoft. Bing Search Engine. https://bing.com/, 2023.

[58] Microsoft. Copilot: Your everyday AI companion. https://copilot.microsoft.com/, 2023.

[59] P. V. Mockapetris. Domain names - concepts and facilities. *RFC*, 1034:1–55, 1987.

[60] P. V. Mockapetris. Domain names - implementation and specification. *RFC*, 1035:1–55, 1987.

[61] Nexus. How to Use ChatGPT to Write an Article. https://nexusmktg.com/use-chatgpt-to-write-article/, 2023.

[62] N. Nikiforakis, M. Balduzzi, L. Desmet, F. Piessens, and W. Joosen. Soundsquatting: Uncovering the use of homophones in domain squatting. In S. S. M. Chow, J. Camenisch, L. C. K. Hui, and S. Yiu, editors, *Information Security - 17th International Conference, ISC 2014, Hong Kong, China, October 12-14, 2014. Proceedings*, volume 8783 of *Lecture Notes in Computer Science*, pages 291–308. Springer, 2014.

[63] N. Nikiforakis, S. Van Acker, W. Meert, L. Desmet, F. Piessens, and W. Joosen. Bitsquatting: exploiting bit-flips for fun, or profit? In D. Schwabe, V. A. F. Almeida, H. Glaser, R. Baeza-Yates, and S. B. Moon, editors, *22nd International World Wide Web Conference, WWW '13, Rio de Janeiro, Brazil, May 13-17, 2013*, pages 989–998. International World Wide Web Conferences Steering Committee / ACM, 2013.

[64] NORTHWEST EXECUTIVE EDUCATION. 6 Tips for Using ChatGPT to Brainstorm Better. https://northwest.education/insights/career-growth/6-tips-for-using-chatgpt-to-brainstorm-better/, 2023.

[65] OpenAI. Introducing ChatGPT. https://openai.com/blog/chatgpt, 2022.

[66] OpenAI. Supported countries and territories. https://platform.openai.com/docs/supported-countries, 2023.

[67] OpenAI. Terms of use. https://openai.com/policies/terms-of-use, 2023.

[68] Peng Peng, Zhanhao Chen, Lucas Hu. ChatGPT-Themed Scam Attacks Are on the Rise. https://unit42.paloaltonetworks.com/chatgpt-scam-attacks-increasing/, 2023.

[69] M. Pereira, S. Coleman, B. Yu, M. D. Cock, and A. C. A. Nascimento. Dictionary extraction and detection of algorithmically generated domain names in passive DNS traffic. In M. D. Bailey, T. Holz, M. Stamatogiannakis, and S. Ioannidis, editors, *Research in Attacks, Intrusions, and Defenses - 21st International Symposium, RAID 2018, Heraklion, Crete, Greece, September 10-12, 2018, Proceedings*, volume 11050 of *Lecture Notes in Computer Science*, pages 295–314. Springer, 2018.

[70] V. L. Pochat, T. van Goethem, S. Tajalizadehkhoob, M. Korczynski, and W. Joosen. Tranco: A research-oriented top sites ranking hardened against manipulation. In *26th Annual Network and Distributed System Security Symposium, NDSS 2019, San Diego, California, USA, February 24-27, 2019*. The Internet Society, 2019.

[71] Public DNS. Public DNS Server 2023. https://www.publicdns.xyz/, 2023.

[72] F. Quinkert, T. Lauinger, W. K. Robertson, E. Kirda, and T. Holz. It's not what it looks like: Measuring attacks and defensive registrations of homograph domains. In *7th IEEE Conference on Communications and Network Security, CNS 2019, Washington, DC, USA, June 10-12, 2019*, pages 259–267. IEEE, 2019.

[73] A. Sarabi, T. Yin, and M. Liu. An llm-based framework for fingerprinting internet-connected devices. In M. Montpetit, A. Leivadeas, S. Uhlig, and M. Javed, editors, *Proceedings of the 2023 ACM on Internet Measurement Conference, IMC 2023, Montreal, QC, Canada, October 24-26, 2023*, pages 478–484. ACM, 2023.

[74] F. Sharevski, J. V. Loop, P. Jachim, A. Devine, and E. Pieroni. Talking abortion (mis)information with chatgpt on tiktok. In *IEEE European Symposium on Security and Privacy, EuroS&P 2023 - Workshops, Delft, Netherlands, July 3-7, 2023*, pages 594–608. IEEE, 2023.

[75] M. Sharma, K. Singh, P. Aggarwal, and V. Dutt. How well does GPT phish people? an investigation involving cognitive biases and feedback. In *IEEE European Symposium on Security and Privacy, EuroS&P 2023 - Workshops, Delft, Netherlands, July 3-7, 2023*, pages 451–457. IEEE, 2023.

[76] Similarweb Blog. ChatGPT Starts to Bounce Back in US as School Year Resumes . https://www.similarweb.com/blog/insights/ai-news/chatgpt-character-ai-2/, 2023.

[77] S. F. Spam. Stop forum spam. https://www.stopforumspam.com/, 2023.

[78] Spam List. Spam List. https://joewein.net/spam/spam-bl-b.htm, 2023.

[79] X. Sun, M. Tong, J. Yang, X. Liu, and H. Liu. Hindom: A robust malicious domain detection system based on heterogeneous information network with transductive classification. In *22nd International Symposium on Research in Attacks, Intrusions and Defenses, RAID 2019, Chaoyang District, Beijing, China, September 23-25, 2019*, pages 399–412. USENIX Association, 2019.

[80] H. Suzuki, D. Chiba, Y. Yoneya, T. Mori, and S. Goto. Shamfinder: An automated framework for detecting IDN homographs. In *Proceedings of the Internet Measurement Conference, IMC 2019, Amsterdam, The Netherlands, October 21-23, 2019*, pages 449–462. ACM, 2019.

[81] J. Szurdi, B. Kocso, G. Cseh, J. M. Spring, M. Félegyházi, and C. Kanich. The long "taile" of typosquatting domain names. In K. Fu and J. Jung, editors, *Proceedings of the 23rd USENIX Security Symposium, San Diego, CA, USA, August 20-22, 2014*, pages 191–206. USENIX Association, 2014.

[82] TechHacker. 10 Best ChatGPT Mirror Sites: No Registration & Bypass GEO. https://freepctech.com/chatgpt/chatgpt-mirror-sites/, 2023.

[83] The Guardian. 'Political propaganda': China clamps down on access to ChatGPT. https://www.theguardian.com/technology/2023/feb/23/china-chatgpt-clamp-down-propaganda, 2023.

[84] K. Tian, S. T. K. Jan, H. Hu, D. Yao, and G. Wang. Needle in a haystack: Tracking down elite phishing domains in the wild. In *Proceedings of the Internet Measurement Conference 2018, IMC 2018, Boston, MA, USA, October 31 - November 02, 2018*, pages 429–442. ACM, 2018.

[85] URLHaus. Urlhaus. https://urlhaus.abuse.ch/, 2023.

[86] T. van Den Hout, T. Wabeke, G. C. M. Moura, and C. Hesselman. Logomotive: Detecting logos on websites to identify online scams - A TLD case study. In O. Hohlfeld, G. C. M. Moura, and C. Pelsser, editors, *Passive and Active Measurement - 23rd International Conference, PAM 2022, Virtual Event, March 28-30, 2022, Proceedings*, volume 13210 of *Lecture Notes in Computer Science*, pages 3–29. Springer, 2022.

[87] T. Vissers, T. Barron, T. van Goethem, W. Joosen, and N. Nikiforakis. The wolf of name street: Hijacking domains through their nameservers. In B. Thuraisingham, D. Evans, T. Malkin, and D. Xu, editors, *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017*, pages 957–970. ACM, 2017.

[88] T. Vissers, W. Joosen, and N. Nikiforakis. Parking sensors: Analyzing and detecting parked domains. In *22nd Annual Network and Distributed System Security Symposium, NDSS 2015, San Diego, California, USA, February 8-11, 2015*. The Internet Society, 2015.

[89] C. Whittaker, B. Ryner, and M. Nazif. Large-scale automatic classification of phishing pages. In *Proceedings of the Network and Distributed System Security Symposium, NDSS 2010, San Diego, California, USA, 28th February - 3rd March 2010*. The Internet Society, 2010.

[90] P. Xia, M. Nabeel, I. Khalil, H. Wang, and T. Yu. Identifying and characterizing COVID-19 themed malicious domain campaigns. In A. Joshi, B. Carminati, and R. M. Verma, editors, *CODASPY '21: Eleventh ACM Conference on Data and Application Security and Privacy, Virtual Event, USA, April 26-28, 2021*, pages 209–220. ACM, 2021.

[91] S. Yadav, A. K. K. Reddy, A. L. N. Reddy, and S. Ranjan. Detecting algorithmically generated malicious domain names. In M. Allman, editor, *Proceedings of the 10th ACM SIGCOMM Internet Measurement Conference, IMC 2010, Melbourne, Australia - November 1-3, 2010*, pages 48–61. ACM, 2010.

[92] R. Yamagishi and S. Fujii. An analysis of susceptibility to phishing via business chat through online survey. *J. Inf. Process.*, 31:609–619, 2023.

[93] H. Yang, X. Ma, K. Du, Z. Li, H. Duan, X. Su, G. Liu, Z. Geng, and J. Wu. How to learn klingon without a dictionary: Detection and measurement of black keywords used by the underground economy. In *2017 IEEE Symposium on Security and Privacy, SP 2017, San Jose, CA, USA, May 22-26, 2017*, pages 751–769. IEEE Computer Society, 2017.

[94] R. Yang, X. Wang, C. Chi, D. Wang, J. He, S. Pang, and W. C. Lau. Scalable detection of promotional website defacements in black hat SEO campaigns. In M. D. Bailey and R. Greenstadt, editors, *30th USENIX Security Symposium, USENIX Security 2021, August 11-13, 2021*, pages 3703–3720. USENIX Association, 2021.

[95] K. Yuan, H. Lu, X. Liao, and X. Wang. Reading thieves' cant: Automatically identifying and understanding dark jargons from cybercrime marketplaces. In W. Enck and A. P. Felt, editors, *27th USENIX Security Symposium, USENIX Security 2018, Baltimore, MD, USA, August 15-17, 2018*, pages 1027–1041. USENIX Association, 2018.

[96] J. Zhang, P. A. Porras, and J. Ullrich. Highly predictive blacklisting. In P. C. van Oorschot, editor, *Proceedings of the 17th USENIX Security Symposium, July 28-August 1, 2008, San Jose, CA, USA*, pages 107–122. USENIX Association, 2008.

[97] Y. Zhang, J. I. Hong, and L. F. Cranor. Cantina: a content-based approach to detecting phishing web sites. In C. L. Williamson, M. E. Zurko, P. F. Patel-Schneider, and P. J. Shenoy, editors, *Proceedings of the 16th International Conference on World Wide Web, WWW 2007, Banff, Alberta, Canada, May 8-12, 2007*, pages 639–648. ACM, 2007.

[98] ZoneFiles. Zonefiles. https://zonefiles.io/detailed-domain-lists/, 2023.