Shielding Brands: An In-depth Analysis of Defensive Domain Registration Practices against Cyber-squatting

Ben Chukwuemeka Benjamin*, Jan Bayer§, Simon Fernandez*, Andrzej Duda*, Maciej Korczyński*
*Univ. Grenoble Alpes, CNRS, Grenoble INP, LIG, Grenoble, France
firstname.lastname@univ-grenoble-alpes.fr
§KOR Labs Cybersecurity, Grenoble, France
firstname.lastname@korlabs.io

***Abstract*—In the digital era, establishing a robust online presence is paramount for brand recognition and trust. However, malicious actors may abuse trust in brand domains with cyber-squatting—registering domain names resembling legitimate ones to deceive users. To counter this threat, brand owners defensively register domain names similar to the original ones, but this protection technique results in increased complexity and financial burden. This paper investigates defensive registration strategies by analyzing 370 prominent brands targeted by cyber-squatters. We provide insight into the activities of leading defensive registrars and highlight the insufficient usage of defensive mechanisms provided by ICANN. Our findings reveal the need for stronger defensive strategies and result in recommendations to enhance brand protection against cyber-squatting.**

***Index Terms*—DNS, Cyber-squatting, Defensive Registration, Passive DNS, WHOIS**

I. Introduction

A well-chosen and relevant domain name is crucial for brand recognition and online presence. Brand owners strive to align their brand names with their domain names to ensure consistency and recognition, which enhances their identity, boosts user trust, and ultimately leads to greater success for the brand. However, malicious actors may abuse the trust in brand domains with cyber-squatting [1] consisting of registering domain names closely resembling the legitimate ones as outlined in the Uniform Domain Name Dispute Resolution Policy (UDRP) defined by ICANN [2]. Variations of cyber-squatting include misspelling, hyphenation, or TLD swaps (the use of different top-level domains) [1], [3]–[5]. For instance, if a company owns the **`brand.com`** domain, miscreants may register **`bramd.com`**, **`brand.xyz`**, or **`brend.com`**.

There are multiple goals of cyber-squatting, for instance serving third-party advertisements, monetizing incoming traffic, or conducting phishing attacks [1], [6].

To protect brands from cyber-squatting, their owners adopt a technique known as *domain name defensive registration*, which involves registering domain names similar to the original ones, primarily to protect a brand from exploitation by malicious actors. However, defensive registration comes with an increased level of complexity: organizations must identify potential domain names for defensive registration and, once registered, monitor their expiration dates, maintain up-to-date contact information for each domain, and secure them (e.g., by configuring strict SPF and DMARC rules to prevent email spoofing [4]). Neglecting these tasks may result in the loss of domain names and takeover by malicious actors, among other risks. Moreover, registering multiple domains may lead to a significant financial burden, especially for small organizations with large brand portfolios to protect [7]–[9].

Given the complexity involved in defensive registrations, brand owners typically rely on third-party providers known as *defensive registrars* such as MarkMonitor [10] or Com Laude [11]. Nevertheless, the defensive registrars face similar challenges to those encountered by brand owners.

This paper investigates defensive registration strategies and analyzes the complexities associated with the protection techniques. We study defensive registrations with an approach that consists of identifying 370 prominent online brands targeted by phishers. From the primary domain names of the brands, we generate over 2.3 M related effective second-level labels (e2LL) by using various methods such as typosquatting, homoglyphs, combosquatting, or TLD swaps. Then, we use the Farsight passive DNS (pDNS) feed [12] to examine the DNS traffic related to the domain names containing the generated e2LLs. We also collect WHOIS data and analyze the reports of disputed domain names. Based on the gathered data, we study the domain name registration activities carried out by leading defensive registrars acting on behalf of brand owners. The activities encompass various aspects such as the types of registered domains, registration timeliness, legal disputes, and the usage of the two types of sunrise periods defined by ICANN: **`End Date Sunrise`** and the **`Start Date Sunrise`** [13]. The periods serve to regulate domain registration, decrease phishing risks, and safeguard the intellectual property rights of brand owners.

As a result of our findings, we propose recommendations to strengthen the strategies used by defensive registrars, particularly relevant in light of the next round of the New gTLD

978-3-903176-64-5

Program announced by ICANN [14].

The main contributions of the paper are as follows:

1) We show that defensive registrars do not take maximum advantage of the **Sunrise** and **Claims** phases for new generic TLDs (ngTLDs), wherein trademark holders can preemptively register domains matching their brands and receive alerts about possible trademark violations.
2) We observe that the **Start Date Sunrise** period type is more effective in terms of covering defensively registered domains (68.2% of studied domain names) during the **Sunrise** and **Claims** phases in comparison to the **End Date Sunrise** type (31.3% of studied domains).
3) We present a new measurement method based on pDNS data to identify the domain names related to brands that could be registered defensively and at what priority.

To the best of our knowledge, this paper is the first study to critically examine the defensive registration activities of major defensive registrars and suggest ways to improve them.

II. Background

This section provides essential background on defensive registration and various cyber-squatting methods.

A. Defensive Registration

Defensive registrars are organizations that provide a comprehensive suite of domain protection services that include identifying and registering variations of domains on behalf of brand owners. If impossible, brand owners can legally challenge entities registering confusingly similar domain names [15], [16].

The legal cases refer to the Lanham Act [17]—a federal statute that governs trademarks, service marks, and unfair competition in the United States. One of its main purposes is to address the issue of *identical or confusingly similar* trademarks. Based on the Lanham Act, ICANN has established the guidelines for the legal dispute proceedings related to the domain name ownership through the Uniform Domain Name Dispute Resolution Policy (UDRP) [18].

Another mechanism set up by ICANN is the Trademark Clearinghouse (TMCH) [19], a centralized database for brand owners to protect their intellectual property rights in the context of new generic TLD (ngTLD) launches.[1]

The introduction of a new gTLD involves several phases aimed at an efficient assignment of domain names to brand owners and the reduction of fraudulent activities while ensuring the integrity of brands. In this paper, we focus on the **Sunrise**, **General Availability**, and **Claims** phases of the sunrise periods [13]. During the **Sunrise** phase, a TLD registry receives the applications for domain name registrations from brand owners or defensive registrars. During the **General Availability** phase, domain names under ngTLDs are made accessible for public registration. Within the initial 90 days of **General Availability**, TLDs are required to undergo a **Claims** phase [21]. If somebody attempts to register a domain containing a trademark verified by TMCH, the registrant receives a warning about potential infringements. Should the domain still be registered, the Trademark Clearinghouse notifies the relevant brand holders of the domain registration, enabling them to take appropriate action. After this period, automatic reporting is not mandatory, and brand owners must activate it themselves.

ICANN established two types of sunrise periods that TLD registries have the authority to choose from: the **End Date Sunrise** and the **Start Date Sunrise** type. When the TLD registry opts for the **End Date Sunrise** type, it must uphold the **Sunrise** phase for a minimum of 60 days. If multiple claims arise for the same domain, auctions determine the winning bidder who will obtain the domain ownership. If the TLD registry opts for the **Start Date Sunrise** type, it must remain active for at least 30 days. The TLD registry processes claims by brand owners on a first-come-first-served basis, thus eliminating the auctions, which implies that domain names are allocated throughout the **Sunrise** phase of the **Start Date Sunrise** type.

Both allocation approaches for domain name registrations may lead to disputes among brand owners and other registrants. To streamline this process and avoid lengthy legal battles, ICANN defined the UDRP rules to simplify the conflict resolution process. They involve trusted legal organizations such as the World Intellectual Property Organization (WIPO) [22] acting as the dispute resolution service provider and appointing panellists from different countries. The UDRP reports contain the details about the involved domains, the complainant (trademark owner), the respondent (violating registrant), the evaluation of cyber-squatting, and the panel decision with its date. According to the UDRP policy, the decision is implemented ten business days from the decision date, unless the respondent files a lawsuit against the complainant [2].

B. Cyber-squatting

Cyber-squatting techniques used by criminals result in generated domain names that may be preemptively acquired by defensive registrars on behalf of their brand owners to mitigate domain name abuse.

1) Typo-squatting: It involves registering domains similar to legitimate brands with intentional typos or letter variations. Its main goal is to deceive users who make typing mistakes when entering a website URL. Exploiting common typing errors like misspellings, transpositions, or omissions, typo-squatters aim to capitalize on traffic intended for a target domain owned by another entity [23]–[27]. For example, in the case of **facebook.com**, attackers may register a confusingly similar domain such as **dacebook.com** [28].

2) Combo-squatting: It consists of registering domain names that combine a popular brand name with deceptive keywords such as **login-facebook.com**, or **facebook-original.com**. According to Kintis et al. [6], combo-squatting differs from other forms of cyber-squatting

[1] As of November 30, 2023, ICANN delegated 1241 ngTLD, such as **.top**, **.xyz**, or **.paris** [20].

because it does not alter the original brand spelling and preserves the original domain while adding words or characters [6], [29]. It makes it challenging for unsuspecting users to verify the authenticity of a combo-squatting domain [29].

3) TLD Swap: It refers to the practice of replacing the TLD of a domain name with a different TLD while preserving the e2LL of the brand, for instance, changing the domain name from **`google.com`** to **`google.zip`**.

4) Homoglyph: Also known as homographs, it is a technique used by malicious actors to register domain names that visually mimic legitimate ones by employing homoglyphs, the characters that look similar but have different Unicode code points. For example, a homoglyph domain may use characters that closely resemble those of a legitimate domain, such as the Greek letter **o** (Unicode U+039f) in **`google.com`**.

5) Bit-squatting: It takes advantage of the possibility of single-bit flip errors in computer memory or network transmission. Miscreants register domains that differ from legitimate ones by only one bit, exploiting potential errors in communication or memory systems. The bit-flips occur due to faulty hardware, or extreme temperatures, and they are thus by nature rare and unpredictable [30], [31]. According to the study by Dinaburg [31], malicious actors registered 30 domains through bitsquatting to target well-known authoritative domains, e.g., **`mic2osoft.com`** (**`2`**: binary **`0011 0010`**) for the benign **`microsoft.com`** domain (**`r`**: binary **`0111 0010`**).

III. Methodology

We first outline our methodology for collecting the datasets investigated in our study. The data flow diagram in Figure 1 illustrates four main processes (① to ④) and two primary external data sources: phishing blocklists and Farsight pDNS.

A. Selection of Brand Domain Names

First, we compile a list of well-known brands frequently targeted by phishing attacks (e.g., Amazon, Microsoft, or Instagram) from three reputable blocklist service providers: the Anti-Phishing Working Group (APWG) [32], PhishTank [33], and OpenPhish [34]. Our analysis of metadata from the blocklists in August 2023 resulted in 370 brand names predominantly targeted by malicious actors in phishing attacks.

B. Effective 2nd Level Label (e2LL) Names

We take the dataset of brand names as input into our candidate e2LL generation algorithm derived by customizing **`dnstwist`** [35] to generate variations of each brand name. We use typo-squatting (addition, insertion, omission, repetition, replacement, vowel-swap, transposition) as well as the **`www+brandname`**, homoglyphs, bitsquatting, and homophones functions. We further extended our list by including combo-squatting candidates generated from the list of 179 keywords that phishers commonly include in domains such as **`secure`**, **`login`**, or **`support`** [6], [36], [37]. The generated list contains 2,303,087 e2LL associated with the 370 targeted brand names.

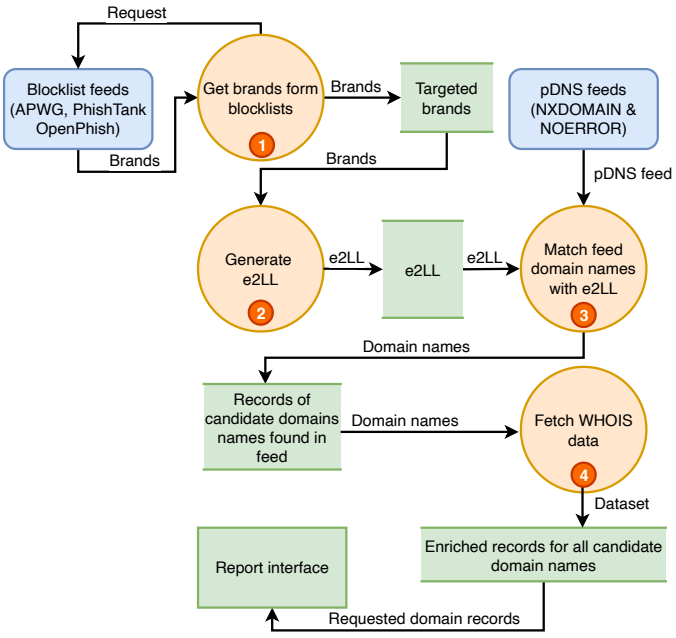

Fig. 1: Data flow diagram of the methodology for collecting datasets.

C. Passive DNS (pDNS) Data

Passive DNS involves observing DNS traffic with sensors placed above recursive resolvers [38] to monitor the queries exchanged between a local resolver and authoritative name servers. The collected local queries are then aggregated into feeds accessible for analysis. We use Farsight Security pDNS [12], and in particular, near-real-time data streams from August 2023 spanning one month, focusing on the 208 **`NOERROR`** and 221 **`NXDOMAIN`** (Non-Existent Domain) channels. For each observed fully qualified domain name (FQDN), we extract effective second-level domain names[2] using the Public Suffix List (PSL) [39]. We obtain registered and non-existing domains containing the enumerated labels.

Note that the observation of certain domains in the **`NXDOMAIN`** channel implies that they are not present in the zone, but they may still be registered without being delegated. Thus, we perform additional WHOIS scans described below.

We found 1,688,194 domains whose labels matched our candidate e2LLs from the **`NXDOMAIN`** and **`NOERROR`** channels.

D. WHOIS Data

WHOIS data contains contact information for a registrar, creation and expiration dates, etc. They can be used for domain-related issues such as potential purchases, legal matters, or technical concerns. To enhance our dataset, we collected WHOIS data for the domain names obtained from the pDNS feeds. We extract the registrar name, its Internet Assigned Numbers Authority (IANA) ID, and the creation date, crucial for identifying the specific phase (**`Sunrise`**, **`General`**

[2]E.g., from **`www.domain.com`** and **`product.domain.co.uk`** we extract **`domain.com`** and **`domain.co.uk`**

TABLE I: Defensive registrars.

Registrar name	IANA ID
AppDetex/Focus IP, dba AppDetex [40]	3235
Com Laude/Nom-IQ Limited [11]	470
CSC Corporate Domains [41]	299
GoDaddy Corporate Domains [42]	3786
Hogan Lovells [43]	1526
IP Twins [44]	1728
MarkMonitor [10]	292
Nameshield [45]	1251
RegistrarSEC/RegistrarSafe [46]	2475/3237
SafeBrands [47]	1290
Safenames [48]	447

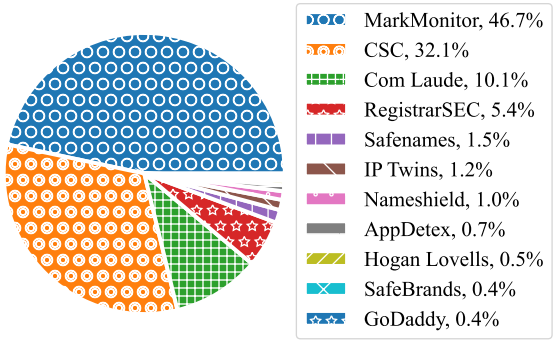

Fig. 2: Percentage of domains registered by each defensive registrar.

Availability, or **Claims**) during which the domain name was registered. We collected the WHOIS data for 407,451 domain names registered by defensive registrars (of which 384,999 came from the **NOERROR** channel and 22,452 from the **NXDOMAIN** channel) and analyzed their registration patterns.

Most domain names in the **NXDOMAIN** channel are unregistered (1,167,472). However, some **NXDOMAIN** returns were registered but not delegated, as indicated by WHOIS scans. In the **NOERROR** channel, errors like timeouts or rate limits prevented data collection for 113,271 domain names.

E. Defensive Registrars

To pinpoint defensively registered domains, we selected eleven reputable and widely recognized defensive registrars known for their partnerships with prominent companies (see Table I). Any domain registered with a registrar listed among them, determined by the IANA ID obtained from WHOIS, was eligible for further analysis.

F. Sunrise Period Analysis

We determined the type of the sunrise period, i.e., the **End Date Sunrise** or **Start Date Sunrise**, and the respective time frames for each phase, i.e., the **Sunrise**, **General Availability**, and **Claims**, using the information published by ICANN [49]. We then compared the timelines with the registration dates of the investigated domain names gathered from WHOIS data.

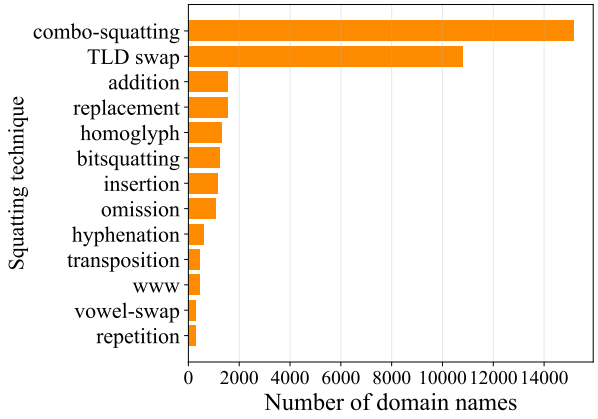

Fig. 3: Distribution of squatting types for all domain names registered by defensive registrars.

G. Identifying Domains for Defensive Registration

Our method for identifying domain names potentially requiring brand protection involves using the pDNS **NXDOMAIN** channel to cross-reference queried non-existent domain names with labels linked to brand names.

To mitigate the risk of accidental collisions between brands and domain names, we analyze domains having at least 5 characters as outlined in previous work [1], [27], [50]. Finally, we sort the candidate domain names based on the number of DNS query counts observed in the pDNS **NXDOMAIN** channel, which, as per WHOIS scans, are unregistered, and map them to their respective brands.

H. Disputed Domain Name Data

We also analyze the domains acquired through legal disputes and associated legal actions. We adopt the same procedure as proposed by Bayer et al. [51] to obtain the data from 4 dispute resolution service providers: WIPO [22], the Alternative Dispute Resolution (ADR) Forum [52], Asian Domain Name Dispute Resolution Center (ADNDRC) [53], and Canadian International Internet Dispute Resolution Center (CIIDRC) [54].

Our analysis solely considers the UDRP reports that have undergone complete execution. More specifically, our evaluation requires that the decision date of the report precede the measurement date by at least 30 days. We check if the complainant associated with each domain listed in the UDRP reports is one of the brands under consideration. If we can successfully identify a brand, we extract the creation date from the WHOIS data of the disputed domain, if available. We have extracted a set of 135,043 unique disputed domain names.

IV. Results

In this section, we examine the registration strategies of top defensive registrars, focusing on their usage of the two types of sunrise periods, domain types, and legal disputes.

Fig. 4: Comparison of the registration pattern by 4 top defensive registrars. RegistrarSec and Com Laude registered more TLD swap domain names, while MarkMonitor and CSC registered more combo-squatting domain names.

A. Registration Patterns by Defensive Registrars

We have identified 36,027 domains (out of which 30,138 are under ngTLDs) registered by the eleven defensive registrars. As shown in Figure 2, 46.7% of domain names are defensively registered exclusively with MarkMonitor, and 94.3% of all studied domain names are registered with only four registrars (MarkMonitor, RegisterSEC, CSC, and Com Laude). As shown in Figure 3, defensive registrars commonly register combo-squatting, TLD swap, and typo-squatting (addition, insertion, omission, repetition, replacement, vowel-swap, transposition) domains.

To analyze the types of registrations, we compared the four largest registrars using the heat map shown in Figure 4. We can observe that all of them registered domain names in all categories but the most common types were combo-squatting and TLD swap. Our comparison reveals that RegistarSEC and Com Laude registered more TLD swap domains, while MarkMonitor and CSC registered more combo-squatting domains. Notably, CSC predominantly registered combo-squatting domains, which sets it apart from the other registrars.

Overall, our analysis highlights a significant clustering of registered domains among a small subset of defensive registrars and offers initial insights into the most prevalent types of cyber-squatting domain names registered by them.

B. Registrations in the `Start Date Sunrise` Period Type

We now analyze the top four largest defensive registrars specifically focusing on ngTLD domain registrations. Previous research revealed a surge in defensive registrations in ngTLDs as companies increasingly protect their brands to prevent abuse [55]. We specifically target 13 prominent brands, including Facebook, Twitter, and Amazon. Figure 5 shows the registration timeline for the **`End Date Sunrise`** period type and its two phases: **`Sunrise`** and **`Claims`**.

We observe that defensive registrars allocated approximately 1.4% of total registrations to multiple brands during the **`Sunrise`** phase. A few registrations are expected in this phase because in the **`End Date Sunrise`** period, registries generally gather applications, and then, the domains with multiple applicants are auctioned to the highest bidder.

The aggregate number of domain name registrations during the **`Sunrise`** and the **`Claims`** phases amounted to around 31.3% of the total registered domain names.

Consider the example of Apple Inc. that registered various ngTLD domains such as **`applewallet.cam`**, **`apple.cam`**, **`iphoto.cam`**, **`isight.cam`**, **`mac.cam`**, **`appleid.cam`**, **`retina.cam`**, and **`icloud.cam`** during the **`Sunrise`** phase. After several days, during the **`Claims`** phase, Apple also registered **`imessage.cam`**, **`imessage.chat`**, and **`imessages.chat`**. However, not all domain names are registered defensively during the **`Sunrise`** and **`Claims`** phases. Apple released a product called **`HomeKit`**, also known as **`Apple Home`**, on September 17, 2014. It took Apple over five and a half years, since the start of the **`Sunrise`** phase in October 2016, to register the **`applehome.cam`** domain name during the **`General Availability`** phase in June 2022.

As many as 68.7% of the domain name registrations took place after the **`Claims`** phase of the **`End Date Sunrise`** period type. One might expect that defensive registrars would use the **`Sunrise`** and **`Claims`** phases to secure most of their defensively registered domain names. It applies to all brands and defensive registrars, which raises concerns as malicious actors may acquire confusingly similar domains before defensive registrars notice them.

We further looked into the **`Start Date Sunrise`** period type that uses the first-come-first-served approach to allocate domains. Our analysis shows that 37.7% of registrations were made during the **`Sunrise`** phase, in contrast to 1.4% during the **`Sunrise`** phase of the **`End Date Sunrise`** period type shown in Figure 6. Moreover, we observed that 30.5% of registrations occurred during the **`Claims`** phase. When we combine the total number of registrations during both **`Sunrise`** and **`Claims`** phases, we see that 68.2% of domain names were defensively registered, which represents a significant improvement from the 31.3% measured during both **`Sunrise`** and **`Claims`** phases of the **`End Date Sunrise`** period type.

The **`Start Date Sunrise`** period type seems to be more effective in terms of covering defensively registered domains during the **`Sunrise`** and **`Claims`** phases. However, we observe that 86.6% of the ngTLD domains in our dataset were registered under the **`End Date Sunrise`** period type while only 13.4% were registered under the **`Start Date Sunrise`**, which indicates that registries may prefer the **`End Date Sunrise`** to the **`Start Date Sunrise`**. One reason could be that the auction of domain names to the highest bidder may generate more significant revenue for the registries.

Different brands have different attitudes towards defensive registrations, as shown in Figure 5. For example, Amazon appears to have the highest number of defensive registrations (5,520) in comparison to other brands. One of the primary factors driving an increased number of defensive registrations could be the frequency of attacks experienced by the brand. To test our hypothesis, we analyze phishing URLs from PhishTank, OpenPhish, and APWG spanning 2021 to 2024.

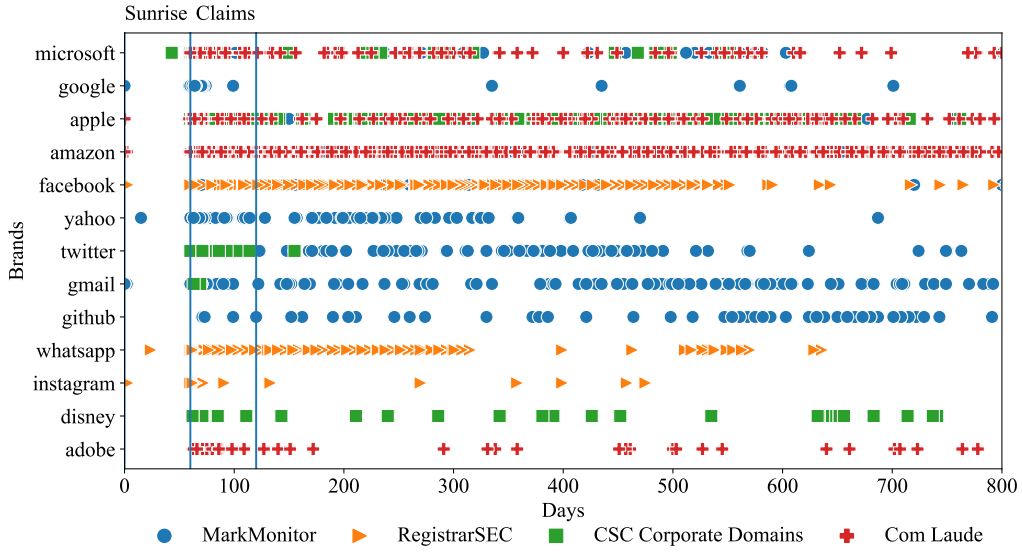

Fig. 5: Registration patterns of ngTLD by MarkMonitor, RegstarSec, CSC, and Com Laude for 13 brands during the **`End Date Sunrise`** period. The majority of registrations occurred following the **`Claims`** phase.

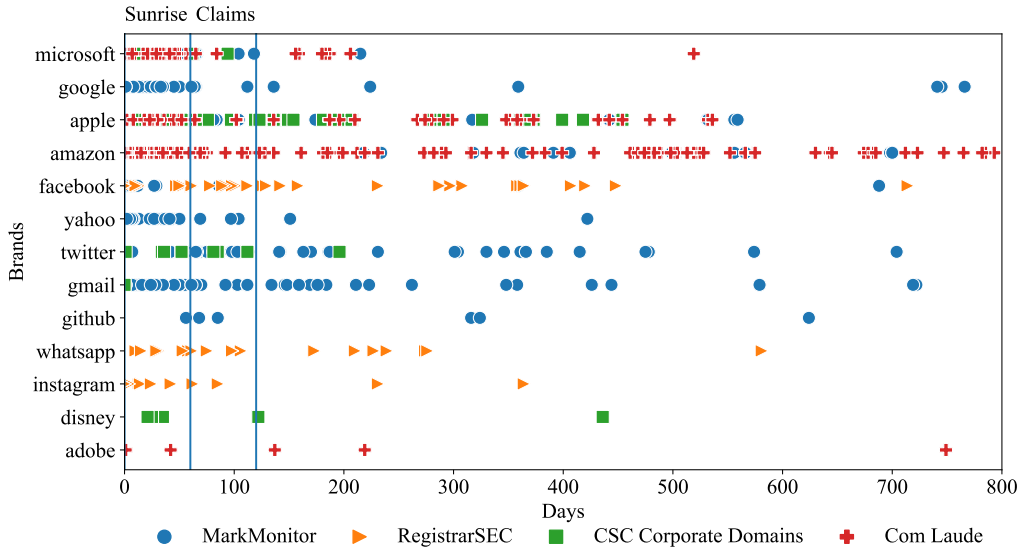

Fig. 6: Registration patterns of ngTLD by MarkMonitor, RegstarSec, CSC, and Com Laude for 13 brands during the **`Start Date Sunrise`** period. Following the **`Claims`** phase, there has been a decrease in defensive registrations.

By removing duplicates based on FQDNs and aligning them with targeted brands from blocklist metadata, we assess the frequency of phishing attacks against defensive registrations. Despite a mix of maliciously registered domains, compromised websites, and free service providers within phishing URLs [36], our findings underscore the focus of attackers on specific brands. As outlined in Section III-G, we consider brand domains with at least 5 characters. Figure 7 reveals a moderately positive relationship (Pearson r = 0.597) between attack frequency and defensive registrations per brand. Nevertheless, outliers exist such as Rabobank with a few phishing attacks captured by blocklists (2 phishing websites), yet demonstrating proactive registration practices (430 defensive registrations).

While we consider the frequency of phishing attacks as a factor influencing defensive registrations, other elements such as specific industry sectors (e.g., banking, social media, etc.) may also be influential. Future research, including regression modeling, could uncover a more comprehensive list of variables contributing to defensive registrations.

C. *Registrations in the* **`End Date Sunrise`** *Period Type*

We now analyze different types of domains registered in the **`Sunrise`** and **`Claims`** phases of the **`End Date Sunrise`**, as well as post-**`Claims`** phase registrations in the **`General Availability`** phase. Out of the total of 162 domains registered in the **`Sunrise`** phase, 137 were TLD swaps, which

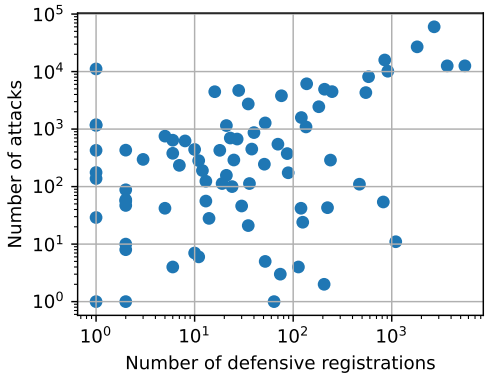

Fig. 7: Scatter plot illustrating the correlation between phishing attacks and defensive registrations for targeted brands.

suggests that registries can allocate these domain names without any concerns regarding ownership legitimacy or waiting for higher bids.

During the **Claims** phase, registries assign the domain names that brand owners have applied for. As shown in Figure 8, 1,494 domain names were registered during the **Claims** phase: they are mostly TLD swaps followed by combo-squatting domains. Defensively registering a TLD swap domain is relatively simple as it only requires adding a TLD to e2LL.

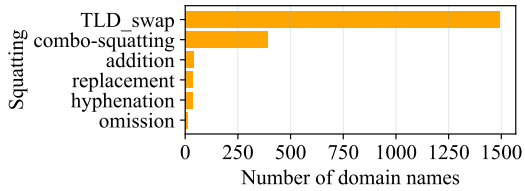

Fig. 8: Types of ngTLD domain names registered during the obligatory **Claims** phase of the **End Date Sunrise** period.

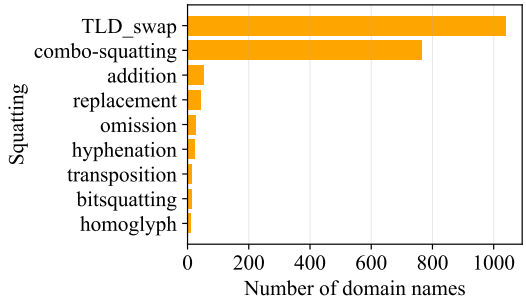

Fig. 9: Types of ngTLD domain names registered after the obligatory **Claims** phase of the **End Date Sunrise** period.

We also examined domains registered after the **Claims** phase required by ICANN, noting 1,041 TLD swaps and 766 combo-squatting instances, with other squatting types each below 100 registered domains (see Figure 9), which contrasts

TABLE II: Examples of ngTLD disputed domain names registered during the **General Availability** phase.

Brand	Disputed domain	Creation	Days after Sunrise
Google	google.pics	2021-05-19	2669
Microsoft	microsoft.services	2015-01-16	262
Twitter	twitter.luxe	2020-10-24	997
Amazon	amazon.watch	2015-01-08	317
Netflix	netflix.store	2017-09-03	515
Apple	apple.works	2016-06-03	822

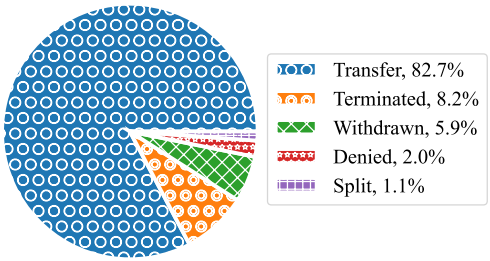

Fig. 10: Decisions on disputed domain names.

with our expectations, as we had assumed that the great majority of TLD swap domains would have been acquired within the **Sunrise** and **Claims** phases. When considering Facebook as a case study, there are notable examples of TLD swap domains that possibly could have been defensively registered during the **Claims** phase. Among these domains are **facebook.photo**, **facebook.events**, **facebook.place**, and **facebook.link**.

D. Domain Names Acquired Through Legal Disputes

Our analysis indicated that miscreants may register confusingly similar domain names before defensive registrars, potentially leading to legal disputes. Reviewing domains involved in such disputes, we found 3,145 linked to 370 brands, with 2,565 registered after the obligatory **Claims** phase. If these registrations had been initiated proactively by brand owners or defensive registrars acting on their behalf, and taken place during the **Sunrise** or **Claims** phases, it might have reduced legal conflicts and protected vulnerable brands. Examples are shown in Table II.

During the **Claims** phase, defensive registrars only registered 37 disputed domain names belonging to top brands. Typically, the individual with the highest bid prevails during the **Claims** phase of **End Date Sunrise** and obtains the desired domain. However, defensive registrars may overlook certain domain names, resulting in third-party registration. If defensive registrars become aware that another party has registered the domain (e.g., via the TMCH notification during the **Claims** phase), they can opt to pursue legal action. Table IV in Appendix B presents some examples of such domains.

We further looked into the outcome of the 3,145 disputed cases related to the 370 brands. We observe that 82.7% (2,602) of the legally disputed domains were successfully transferred

to the defensive registrars (see Figure 10). Disputed transfer decisions revolve around confirming that the respondent registered the confusingly similar domain name in bad faith, in line with UDRP rules [18].

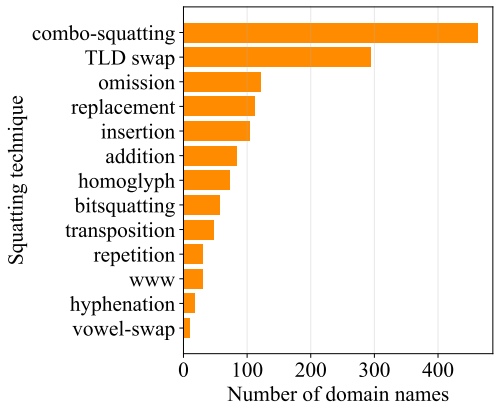

Fig. 11: Types of cyber-squatting associated with disputed domain names with the transfer decision.

Figure 11 highlights combo-squatting and typo-squatting domains (addition, insertion, omission, repetition, replacement, vowel-swap, transposition) as the most prevalent type of transferred domains. While it is difficult to identify and register all combo-squatting domains related to a brand, it is still surprising to see a large number of disputed TLD swap domains. Thus, brand owners may need to strengthen efforts to defensively register those domains before other third parties.

We also observe that 5.9% of the legally disputed domain names were withdrawn. They are the cases for which the defendant decided to hand over the domain to the brand owner willingly (e.g., **`bankofamericaonline.org`**, **`yahoo2.com`**, **`googlegroup.com`**, or **`disny.com`**).

We observe that 2% of the legally disputed domains were denied, which means that the judgment went against the brand owners even though the domain names are identical or confusingly similar to their brands (see Table V in Appendix B for some examples). The panel ruled that brand owners could not substantially prove that the disputed domains were registered and used in bad faith [18]. For example, **`netlix.com`** was registered before the Netflix brand was created.

In some cases, the legal disputes can involve multiple domain names. In a situation in which not all disputed domains are awarded to the brand owner, the decision is referred to as a split decision. The 1.1% split decisions are disputes in which only a portion of the domain names was awarded to the complainant as shown in Table VI in Appendix B.

The remaining 8.2% terminated cases are disputes in which both the complainant and the respondent have to resort to other means of resolving the dispute, which in some cases means that a superior court will have to handle the dispute rather than a domain name dispute resolution center [56].

Preemptive registration of domains may significantly decrease the number of legal disputes facing brand owners. These disputes can be both time-consuming and expensive,[3] and not all disputed cases end in favor of brand owners.

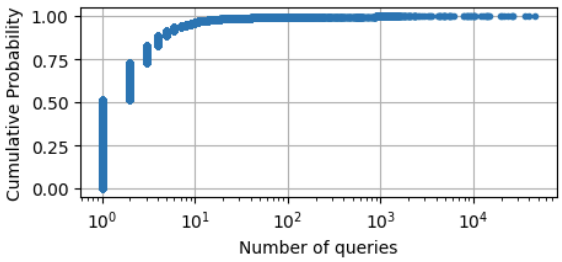

Fig. 12: CDF of domains in the **`NXDOMAIN`** channel ordered by the observed DNS query counts.

TABLE III: Examples of domain names recommended for defensive registration (anonymized).

Domain names	Technique	Queries	Specialty
brand1update.net	combo-squatting	10,110	Software
brand1update.co	combo-squatting	10,106	Software
brand2-maps.app	combo-squatting	35,995	Mobile
music-**brand2**.ru	combo-squatting	8,724	Mobile
world**brand3**.ru	combo-squatting	13,823	Movie
brand4-login.biz	combo-squatting	1,075	Social media
brand5info.com	combo-squatting	9,301	Movie

It remains uncertain whether exhaustive registrations are financially advantageous for brand owners—it would require a thorough estimation of the global costs associated with defensive registrations including prevented financial losses [58] and considering the costs of disputes and losses resulting from the registration of brand names by unintended, potentially malicious users [58].

*E. Analysis of the **`NXDOMAIN`** Channel*

We collected 1,177,737 domains from the pDNS **`NXDOMAIN`** channel, which include e2LLs generated using the method outlined in Section III-B. We only considered domains of at least 5 characters (see Section III-G), thus further reducing the number of domains to 360,874. The gathered WHOIS data indicates that 210,307 domains have not been registered.

The DNS query counts shown in Figure 12 reveal that a substantial number of 209,256 domains exhibit modest counts, falling below 100 queries. At the same time, the remaining 1,051 domains require attention with higher query volumes, ranging from over 100 to as high as 45,883 queries during a single month. Table III presents the examples of domains featuring exact brand names (anonymized) alongside with their DNS query counts.

Note that following our initial measurements, two domains (**brand6**-support.net with 45,883 queries and **brand7**w.com with 558 queries) were registered. After a thorough analysis, we determined that both entities are not affiliated with any of the brands and are not defensive registrars.

[3]e.g., a dispute may cost $1,500 according to the WIPO Fees schedule [57].

Liu et al. [59] used pDNS to detect the domains with a substantial volume of DNS queries, registering 19 of them for the analysis of incoming traffic. It indicates that the bulk of domain visits originate from web crawlers, automated processes, referrals, and user visits. However, it also reveals malicious activity, suggesting exploitation by adversaries. They analyzed the security implications of unintended users registering such domains. For instance, adversaries could establish phishing web pages or inject malicious programs into these domains to carry out harmful activities. Therefore, we argue that such domains should be identified and registered defensively.

We explored the risk of unintended individuals registering domains resembling popular brands by selecting five domains with high DNS query counts. When attempting to register a WhatsApp-related domain with a prominent registrar, it detected the brand name, requesting further details for registration. We then tried another registrar and succeeded. However, within three days, we were asked to provide administrative documents to prove our WhatsApp affiliation. We registered the remaining four domains without problems, which illustrates the ease of acquiring confusingly similar domains containing brand names. It also indicates that outside the **`Claims`** phase, brand owners did not activate security measures like TMCH.

F. Discussion and Recommendations

Our analysis of defensive registration strategies uncovered various obstacles that defensive registrars encounter and the potential consequences they may face. In light of these findings, we suggest that brand owners consider registering all possible TLD swap domains within the **`Sunrise`** and **`Claims`** phases.

Keeping in mind the complexity of identifying potential combo-squatting and typo-squatting domains, defensive registrars could use pDNS combined with our method for analyzing the traffic to non-existent domains similar to brands that have not been claimed by brand owners through defensive registrars.

The brand owners, registrars, and registries could also actively monitor registrations, and identify cyber-squatting attempts, for instance, via TMCH outside the **`Claims`** phase.

Finally, we observe that the **`Start Date Sunrise`** type is more effective in terms of covering defensively registered domains during the **`Sunrise`** and **`Claims`** phases and, therefore, could be a preferred option when delegating ngTLDs.

Nevertheless, the effectiveness and economic impacts of extensive defensive registrations remain uncertain. Attackers may create complex variations of squatting domains or switch to registering random domain names and using deceptive keywords within subdomains. While such domains could potentially be identified through careful passive DNS monitoring, promptly blocking them might only mitigate the harm rather than entirely prevent it.

Another unresolved issue is the cost of thorough defensive registrations during sunrise periods and legal disputes, compared to the challenging task of estimating prevented losses to the brand owner and victims of phishing attacks.

Finally, there remains the question regarding the types of companies and brand owners as well as their sectors that should prioritize the investment in defensive registrations. While the frequency of phishing attacks could offer some initial insight, addressing this question requires identifying numerous potential contributing factors to abuse and conducting a thorough regression analysis assuming a comprehensive coverage of phishing blocklists.

V. Related work

Much research addressed the problem of cyber-squating [1], [5], [6], [23]–[27], [29], [60]. Szurdi et al. [1] investigated the typo-squatting registrations, focusing on their prevalence in the **`.com`** TLD. Kintis et al. [6] only considered domain abuse based on combo-squatting of brands limited to the US and relied on Alexa. Lui et al. [60] examined homoglyphs and Internationalized Domain Names (IDNs) in popular gTLDs. Zeng et al. [29] analyzed the financial implications of domain squatting abuse based on the Alexa list. Quinkert et al. [5] relied on the Majestic list [61] and designed a measurement infrastructure for studying homograph domains. While their work identified defensive registrations, its main focus was on detecting instances of scamming and phishing. To the best of our knowledge, we are the first to investigate thoroughly the issue from the viewpoint of defensive registrars.

Liu et al. [59] used pDNS and registered several domains with a large number of DNS queries. They set up honeypots to capture traffic going to these domains to identify their sources.

Our research overcomes prior limitations by selecting seed domains from reputable blocklists and diverse data sources, which yields valuable insights into defensive registrations and enhances our understanding of brand protection measures.

VI. Conclusions

The paper has delved into the defensive registration strategies used by major defensive registrars and examined the nuances linked with protective measures.

Our analysis reveals that registrars primarily engage in registering combo-squatting, TLD swaps, and typo-squatting for protective purposes. We find that 68.7% (respectively 31.8%) of ngTLD domains were defensively registered during the **`Sunrise`** and **`Claims`** phases of the **`End Date Sunrise`** (respectively, the **`Start Date Sunrise`**). This finding suggests that defensive registrars do not fully capitalize on these phases to protect brands.

Additionally, our results indicate that 82.7% of the studied domains involved in legal disputes were successfully transferred to defensive registrars. However, we argue that preemptive domain registration may significantly mitigate the number of costly legal disputes and not always resolved in favor of brand owners.

Finally, our findings demonstrate that pDNS can serve as a valuable asset for defensive registrars seeking to reinforce their strategies.

Acknowledgments

We would like to thank the anonymous reviewers and our shepherd Raffaele Sommese for their valuable feedback and Sourena Maroofi for his initial input to the paper. We thank Farsight Security/DomainTools for providing access to the passive DNS data. This work has been partially supported by the French Ministry of Research projects PERSYVAL Lab under contract ANR-11-LABX-0025-01, DiNS under contract ANR-19-CE25-0009-01, and Grenoble Alpes Cybersecurity Institute (ANR-15-IDEX-02).

References

[1] J. Szurdi, B. Kocso, G. Cseh, J. Spring, M. Felegyhazi, and C. Kanich, "The Long "Taile" of Typosquatting Domain Names," in *USENIX Security Symposium*, 2014, pp. 191–206.

[2] ICANN, "Uniform Domain Name Dispute Resolution Policy," https://www.icann.org/resources/pages/policy-2012-02-25-en, 1999.

[3] J. Spaulding, S. Upadhyaya, and A. Mohaisen, "The landscape of domain name typosquatting: Techniques and countermeasures," in *ARES*, 2016, pp. 284–289.

[4] S. Maroofi, M. Korczyński, and A. Duda, "From Defensive Registration to Subdomain Protection: Evaluation of Email Anti-Spoofing Schemes for High-Profile Domains," in *TMA*, 2020, pp. 1–9.

[5] F. Quinkert, T. Lauinger, W. Robertson, E. Kirda, and T. Holz, "It's Not What It Looks Like: Measuring Attacks and Defensive Registrations of Homograph Domains," in *IEEE CNS*, 2019.

[6] P. Kintis, N. Miramirkhani, C. Lever, Y. Chen, R. Romero-Gómez, N. Pitropakis, N. Nikiforakis, and M. Antonakakis, "Hiding in Plain Sight: A Longitudinal Study of Combosquatting Abuse," in *ACM SIGSAC*, 2017, pp. 569–586.

[7] E. Goldman, "Why Defensive Domain Name Registrations Aren't a Good Deal for Small Businesses," https://www.forbes.com/sites/ericgoldman/2012/07/16/why-defensive-domain-name-registrations-arent-a-good-deal-for-small-businesses/, 2012.

[8] ICANN, "Defensive Registration - ICANN Wiki," https://icannwiki.org/Defensive_Registration, 2022.

[9] T. Halvorson, K. Levchenko, S. Savage, and G. M. Voelker, "XXXtortion? Inferring registration intent in the .XXX TLD," in *WWW*, 2014, pp. 901–912.

[10] MarkMonitor, "Markmonitor - domain management solutions, domain security," https://www.markmonitor.com/, 1999.

[11] Com Laude, "Corporate Domain Name Management for Brands - Com Laude," https://comlaude.com/, 2004.

[12] Farsight Security, "Passive DNS Historical Internet Database: Farsight DNSDB," https://www.farsightsecurity.com/solutions/dnsdb/, 2022.

[13] ICANN, "Sunrise Period - ICANNWIki," https://icannwiki.org/Sunrise_Period, 2021, (Accessed on 01/22/2024).

[14] ICANN, "Status Update: New gTLD Program: Next Round," https://www.icann.org/en/system/files/files/status-update-new-gtld-program-next-round-20feb24-en.pdf, 02 2024, (Accessed on 04/25/2024).

[15] H. P. Singh, "Domain Name Disputes and Their Resolution under UDRP Route: A Review," *Archives of Business Research*, vol. 6, no. 12, 2018.

[16] D. A. Simon, "An Empirical Analysis of Fair Use Decisions Under the Uniform Domain-Name Dispute-Resolution Policy," *BCL Rev.*, vol. 53, p. 65, 2012.

[17] Legal Information Institute, "Lanham Act," https://www.law.cornell.edu/wex/lanham_act, (Accessed on 11/01/2023).

[18] ICANN, "Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules")," https://www.icann.org/resources/pages/udrp-rules-2015-03-11-en, 2015.

[19] Trademark Clearinghouse, "What is the Trademark Clearinghouse," https://www.trademark-clearinghouse.com/content/what-trademark-clearinghouse, (Accessed on 10/30/2023).

[20] ICANN, "New gTLD Program Statistics," https://newgtlds.icann.org/en/program-status/statistics, 2024.

[21] Trademark Clearinghouse, "What is the Claims Period?" https://trademark-clearinghouse.com/help/faq/what-claims-period.

[22] World Intellectual Property Organization, "WIPO Domain Name Decisions," https://www.wipo.int/amc/en/domains/decisionsx/.

[23] P. Agten, W. Joosen, F. Piessens, and N. Nikiforakis, "Seven Months' Worth of Mistakes: A Longitudinal Study of Typosquatting Abuse," in *NDSS*, 2015, pp. 1–13.

[24] M. T. Khan, X. Huo, Z. Li, and C. Kanich, "Every Second Counts: Quantifying the Negative Externalities of Cybercrime via Typosquatting," in *IEEE SP*, 2015, pp. 135–150.

[25] A. Banerjee, M. S. Rahman, and M. Faloutsos, "SUT: Quantifying and Mitigating URL Typosquatting," *Computer Networks*, vol. 55, no. 13, pp. 3001–3014, 2011.

[26] Y.-M. Wang, D. Beck, J. Wang, C. Verbowski, and B. Daniels, "Strider Typo-Patrol: Discovery and Analysis of Systematic Typo-Squatting," *USENIX SRUTI*, vol. 6, no. 31-36, 2006.

[27] V. Le Pochat, T. Van Goethem, and W. Joosen, "A Smörgåsbord of Typos: Exploring International Keyboard Layout Typosquatting," in *IEEE SPW*, 2019, pp. 187–192.

[28] I. Lunden, "U.S. Court Rules For Facebook In Its Case Against Typosquatters On 105 Domains; $2.8M In Damages," https://techcrunch.com/2013/05/01/u-s-court-rules-for-facebook-in-its-case-against-typosquatters-on-105-domains-2-8m-in-damages/, 2013.

[29] Y. Zeng, T. Zang, Y. Zhang, X. Chen, and Y. Wang, "A Comprehensive Measurement Study of Domain-Squatting Abuse," in *IEEE ICC*, 2019.

[30] T. Vissers, T. Barron, T. Van Goethem, W. Joosen, and N. Nikiforakis, "The Wolf of Name Street: Hijacking Domains Through Their Nameservers," in *ACM SIGSAC CCS*, 2017, pp. 957–970.

[31] A. Dinaburg, "Bitsquatting: DNS Hijacking Without Exploitation," *DEFCON*, 2011.

[32] Anti-Phishing Working Group, "Global Phishing Survey: Trends and Domain Name Use in 2016," https://docs.apwg.org/reports/APWG_Global_Phishing_Report_2015-2016.pdf, 2016.

[33] D. Ulevitch, "PhishTank," https://phishtank.org/, 2006.

[34] OpenPhish, https://openphish.com/, 2023.

[35] M. Ulikowski, "DNSTwist," https://github.com/elceef/dnstwist.

[36] S. Maroofi, M. Korczyński, C. Hesselman, B. Ampeau, and A. Duda, "COMAR: Classification of Compromised versus Maliciously Registered Domains," in *IEEE EuroS&P*, 2020, pp. 607–623.

[37] J. Bayer, B. C. Benjamin, S. Maroofi, T. Wabeke, C. Hesselman, A. Duda, and M. Korczyński, "Operational Domain Name Classification: From Automatic Ground Truth Generation To Adaptation To Missing Values," in *PAM*, 2023, p. 564–591.

[38] F. Weimer, "Passive DNS Replication," https://www.first.org/conference/2005/papers/florian-weimer-paper-1.pdf.

[39] Mozilla, "Public Suffix Lists," https://publicsuffix.org/list/.

[40] Tracer, "Brand Protection Software," https://www.tracer.ai/products/registrar.

[41] CSC, "CSC The Most Security Conscious Domains Provider," https://www.cscdbs.com/en/why-csc/csc-digital-brand-services, 2008.

[42] GoDaddy Inc., "GoDaddy Corporate Domains," https://gcd.com/.

[43] Hogan Lovells, "Domain Names," https://www.hoganlovells.com/en/service/domain-names/.

[44] IP Twins, "Domain Names and Online Brand Protection," https://www.iptwins.com/en/home/.

[45] Nameshield, "Nameshield Secures Your Strategic Domain Names," https://www.nameshield.com/en/.

[46] RegistrarSEC, "RegistrarSEC / RegistrarSafe," https://registrarsec.com/.

[47] SafeBrands, "Safebrands," https://safebrands.com/.

[48] Safenames, "Safenames - Global Domain Search, Registration and Protection," https://www.safenames.net/.

[49] ICANN, "TLD Start Information," https://newgtlds.icann.org/en/program-status/sunrise-claims-periods, 2015, (Accessed on 04/25/2024).

[50] T. Moore and B. Edelman, "Measuring the perpetrators and funders of typosquatting," in *Financial Cryptography*, 2010, pp. 175–191.

[51] B. Jan, M. Sourena, H. Olivier, D. Andrzej, and K. Maciej, "Building a Resilient Domain Whitelist to Enhance Phishing Blocklist Accuracy," in *eCrime*, 2023.

[52] ADR Forum, "Domain Name Dispute Proceedings & Decisions," https://www.adrforum.com/domain-dispute/search-decisions.

[53] Asian Domain Name Dispute Resolution Center, "UDRP Decisions," https://www.adndrc.org/decisions/udrp, (Accessed 23-May-2023).

[54] Canadian International Internet Dispute Resolution Center, "CIIDRC Decisions," https://ciidrc.org/domain-name-disputes/ciidrc-decisions/, (Accessed 23-May-2023).

[55] T. Halvorson, M. F. Der, I. Foster, S. Savage, L. K. Saul, and G. M. Voelker, "From .Academy to .Zone: An Analysis of the New TLD Land Rush," in *ACMIMC*, 2015, pp. 381–394.

[56] WIPO, "An International Guide to Patent Case Management for Judges," https://www.wipo.int/patent-judicial-guide/en/full-guide/republic-of-korea/8.6.2, (Accessed on 01/15/2024).
[57] WIPO, "Schedule of Fees under the UDRP," https://www.wipo.int/amc/en/domains/fees/, (Accessed 11/01/2023).
[58] R. Anderson, C. Barton, R. Böhme, R. Clayton, M. J. G. van Eeten, M. Levi, T. Moore, and S. Savage, *Measuring the Cost of Cybercrime*. Springer Berlin Heidelberg, 2013, pp. 265–300.
[59] G. Liu, L. Jin, S. Hao, Y. Zhang, D. Liu, A. Stavrou, and H. Wang, "Dial "N" for NXDomain: The Scale, Origin, and Security Implications of DNS Queries to Non-Existent Domains," in *ACM IMC*, 2023.
[60] 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 *IEEE/IFIP DSN*, 2018, pp. 654–665.
[61] Majestic, "The Majestic Million," https://majestic.com/reports/majestic-million, 2019.
[62] D. Dittrich and E. Kenneally, "The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research," https://catalog.caida.org/paper/2012_menlo_report_actual_formatted, 2012.
[63] C. Partridge and M. Allman, "Ethical Considerations in Network Measurement Papers," *Commun. ACM*, vol. 59, no. 10, p. 58–64, 2016.

APPENDIX

A. Ethical Considerations

We carefully crafted our methodology to address ethical considerations when conducting network measurements [62], [63].Throughout the collection of the WHOIS data, we have consistently adhered to the query limits and dispersed our scans over 30 days.

Farsight pDNS data is deliberately aggregated in a way that protects data privacy. We have anonymized certain e2LL of unregistered domain names to ensure that unintended users do not register them.

For the registered domain name sample, we did not set up DNS and web servers to collect user data, and we listed our contact details on WHOIS, enabling brand owners or defensive registrars to contact us if they are interested in acquiring them.

B. Examples of Disputed Domain Names

We present examples of domain names registered by an external entity during the **`Claims`** phase and disputed by brand owners in Table II. Table V shows disputed domain names for which defensive registrars were denied transfer. During a domain name dispute, some names may be transferred to brand owners while others are not, as shown in Table VI.

TABLE IV: Examples of disputed domain names with the targeted brand registered during the **`Claims`** phase.

Brand	Disputed domains	Creation	Days after Sunrise
Alibaba	alibaba.careers	2014-04-13	110
Yahoo	yahoosupport.tech	2015-08-24	91
Walmart	walmart.lgbt	2015-05-11	126
Walmart	walmart.reviews	2017-09-03	98
Carrefour	carrefour.company	2014-03-20	79

TABLE V: Examples of disputed domain names for which defensive registrars were denied transfer.

Brand	Disputed domain name	Reason
Netflix	netlix.com	netlix.com was registered before the netflix brand was created.
Google	oogle.com, woogle.com	Complainant could not prove that oogle.com was used in bad faith.
Metamark	metamark.com	Complainant could not prove that metamark was used in bad faith.
PayPay	paypay.com	Complainant lacks the proper jurisdiction
America Online	aol-city.com	Respondent proved to have a genuine reason to use the letter **`aol`** in their domain name.
Coinbase	coinbase.info	Respondent have legitimate rights in COINBASE resulting from the Chinese registrations.

TABLE VI: Examples of disputed denied domain names involved in a split decision case.

Brand	Denied domain	Denied	Transfered
Twitter	twitter-supported.com	1	2
Coinbase	coinbase.net	1	2
Google	gtmail.com	1	33
Google	goojle.com	18	110
America Online	aolc.com	10	15