Registration, Detection, and Deregistration: Analyzing DNS Abuse for Phishing Attacks

Kyungchan Lim
University of Tennessee
Knoxville, USA
klim7@utk.edu

Raffaele Sommese
University of Twente
Enschede, The Netherlands
r.sommese@utwente.nl

Mattijs Jonker
University of Twente
Enschede, The Netherlands
m.jonker@utwente.nl

Ricky Mok
CAIDA/UC San Diego
San Diego, USA
cskpmok@caida.org

kc claffy
CAIDA/UC San Diego
San Diego, USA
kc@caida.org

Doowon Kim
University of Tennessee
Knoxville, USA
doowon@utk.edu

arXiv:2502.09549v2 [cs.CR] 17 Apr 2025

Abstract

Phishing continues to pose a significant cybersecurity threat. While blocklists currently serve as a primary defense, due to their reactive, passive nature, these delayed responses leave phishing websites operational long enough to harm potential victims. It is essential to address this fundamental challenge at the root, particularly in phishing domains. Domain registration presents a crucial intervention point, as domains serve as the primary gateway between users and websites.

We conduct a comprehensive longitudinal analysis of 690,502 unique phishing domains, spanning a 39-month period, to examine their characteristics and behavioral patterns throughout their lifecycle—from initial registration to detection and eventual deregistration. We find that 66.1% of the domains in our dataset are maliciously registered, leveraging cost-effective TLDs and targeting brands by mimicking their domain names under alternative TLDs (*e.g.*, `.top` and `.tk`) instead of the TLDs under which the brand domains are registered (*e.g.*, `.com` and `.ru`). We also observe minimal improvements in detection speed for maliciously registered domains compared to compromised domains. Detection times vary widely across blocklists, and phishing domains remain accessible for an average of 11.5 days after detection, prolonging their potential impact. Our systematic investigation uncovers key patterns from registration through detection to deregistration, which could be leveraged to enhance anti-phishing active defenses at the DNS level.

1 Introduction

Phishing attacks continue to pose one of the most pervasive cybersecurity threats, with attackers deploying increasingly sophisticated impersonation tactics. The attackers create convincing replicas of legitimate websites (*e.g.*, `facebook.com` or `USPS.com`), to deceive users into divulging their login credentials and sensitive information. Such attacks have substantial consequences, leading to financial losses for victims [1], reputational harm for impersonated organizations [8], and compromised business infrastructures [46].

The blocklisting mechanisms (*e.g.*, Google Safe Browsing [24]) currently serve as the primary defense against phishing attacks. Google Safe Browsing is integrated into Google Chrome browsers and by default enabled for end-users. These systems aim to protect users by preventing access to known (*i.e.*, blocklisted) phishing websites. However, their reactive (*i.e.*, passive) nature introduces critical security gaps in phishing protection. The fundamental limitation of blocklists lies in their update latency—the time gap between when attackers register domains and deploy a new phishing site and when security crawlers detect, verify, and add it to the blocklist. This delay creates a vulnerability window during which new phishing sites remain accessible to potential victims, allowing attackers to freely operate their campaigns. Notably, a previous work [51] indicated that 75% of victims may encounter the malicious site before blocklist updates take effect.

To effectively combat phishing attacks, it is essential to address the fundamental problem at the root, particularly phishing domains. Domains play a pivotal role in connecting users to websites, including malicious ones. This critical position makes domains an ideal intervention point for detecting and preventing phishing attacks before they can reach potential victims. Particularly, phishing attackers can choose between two strategies for utilizing domain names: 1) registering a new domain specifically for malicious purposes; or 2) compromising an existing, legitimate website with an already established domain. Maliciously registered domains present a unique opportunity for mitigation at the domain level, as these domains are intentionally created to facilitate malicious activities.

Prior studies [28, 44, 46, 48, 49, 51] have explored various aspects of phishing websites, such as ccTLD, URL patterns and visual content. Specifically, Moura et al. [46] analyzed phishing domains mimicking target brand webpages but focused solely on three European ccTLDs: `.nl`, `.ie`, and `.be`. While Maroofi et al. [44] introduced the methods to define maliciously registered domains, the characteristics of maliciously registered domains for phishing attacks have been unexplored. Despite the importance of understanding the dynamic behaviors and lifecycle of maliciously registered domains, these aspects remain largely unexamined to date.

To address this gap, our study undertakes a systematic, longitudinal analysis of phishing attacks using phishing domains, with a focus on those that are maliciously registered domains. By examining these phishing domains from registration to detection and eventual deregistration, we aim to better understand the phishing attack ecosystem at the domain level. To further understand maliciously registered domains, we raise the two following research questions. **RQ1:** *What are the characteristics of maliciously registered domains and how can we find maliciously registered domains?* **RQ2:** *What is the lifecycle of a maliciously registered domain?*

Our analysis shows that 66.1% of all names in our phishing domains dataset are specifically registered for malicious purposes. To better understand these malicious domains, we examine their characteristics, focusing on TLD usage and targeted brands. We observe that new gTLDs (*e.g.*, `.top`, `.shop`) are widely utilized due to their low cost (as little as $1 per domain). Following the cessation of Freenom, the use of the `.cn` TLD increased significantly. Notably, the `USPS` brand experienced a sharp rise in domain registrations, frequently under cost-effective TLDs. The latter holds true for `Ozon` as well. Our observations align with prior research [32].

To gain deeper insights into phishing domains with malicious registration activity, we analyze their DNS records, dynamic behavior, and lifespan, spanning from registration to detection and eventual deregistration. Our analysis reveals that phishing domains often exhibit dynamic DNS behavior, frequently updating their DNS records with short TTLs, indicative of fast-flux DNS techniques. Regarding lifespan, maliciously registered domains are detected slightly faster than compromised domains with a median detection time of 16.3 days for malicious domains compared to 86 days for compromised domains. On average, deregistration occurs approximately 11.5 days after detection. However, detection delays vary significantly across blocklists, with some domains listed in `Phishing.Database` showing an average detection delay of up to 388.5 days.

Our contributions are as follows:

- Building on previous methods, we enhance the approach to identify maliciously registered domains. Our analysis reveals that 66.1% of the domains in our dataset are maliciously registered, with the remainder being compromised domains.
- From our analysis of maliciously registered domains in our dataset, we identify three key characteristics: 1) New gTLDs: Domains frequently use low-cost new gTLDs (*e.g.*, `.top`, `.xyz`, and `.online`), with `.cn` usage rising after Freenom ceased free registrations [38], aligning with previous reports [32]. 2) TLD Variation in Brand Targeting: Phishing domains targeting brands (*e.g.*, `USPS`, `OZON`) often use alternative TLDs (*e.g.*, `.top`, `.tk`) instead of the brand's original TLDs (*e.g.*, `.com`, `.ru`). 3) DNS Fast Flux: 64.3% of domains show frequent DNS updates, with 25.8% using TTLs below 3600 seconds to possibly enable DNS fast flux.
- We find that maliciously registered domains are detected by blocklists (*e.g.*, APWG) faster than compromised domains, with a median detection time of 16.3 days for malicious domains compared to 86 days for compromised domains. Additionally, detection times vary significantly across blocklists, with USPS and Ozon being the quickest with 1.4 and 1.3 days respectively. Even after detection by blocklists (*e.g.*, APWG), phishing domains remain accessible for an average of 11.5 days, prolonging the risk to potential victims.
- We present a comprehensive longitudinal analysis of phishing domains (39 months). We publicly share our collected phishing dataset (*i.e.*, phishing domains) to facilitate future phishing research upon acceptance.

2 Background

We provide a brief overview of domain registration and DNS records, with an emphasis on phishing attacks.

2.1 Domain Registration and DNS Record

Domain Registration. Domain registration is the foundational process through which a unique domain name is acquired and associated with an individual or organization. This process involves selecting a domain name and choosing a top-level domain (TLD), such as `.com`, `.org`, or country-specific TLDs, such as `.us` or `.cn`. Once a domain is registered through a registrar, critical DNS records—such as A records, which link the domain to an IP address, and NS records, which designate authoritative name servers—are established to facilitate the Web services. The registry maintains the TLD's zone file, which includes delegation details for domains under that TLD. These zone files are updated in real-time or periodically by the registry as domain registrations and configurations change. Separately, organizations like ICANN collect published snapshots of these zone files at regular intervals (*e.g.*, every 24 hours for gTLDs [31]), though the exact frequency depends on the TLD administrator's policies. It's important to note that the frequency of published zone file snapshots is distinct from the registry's internal updates to the zone file.

WHOIS. Registration data is typically accessed through WHOIS or the Registration Data Access Protocol (RDAP). WHOIS has been the standard for retrieving domain registration information since the 1970s. However, due to its inconsistencies and limitations, RDAP was introduced in 2015 as its successor. RDAP improves upon WHOIS by offering structured, machine-readable registration data along with advanced features such as differentiated access, internationalization, and extensibility. By examining the domain registration choices of phishing sites, including their TLD preferences, registrar selection, and DNS configuration, researchers can uncover patterns that may inform more effective, proactive detection methods against these evolving threats.

Top-level Domain (TLD). As described in prior work [30], gTLDs can be categorized into legacy gTLDs and new gTLDs. New gTLDs refer to TLDs introduced as part of ICANN's expansion program in 2012. Initially, there were only 8 gTLDs, and another 8 in 2004. In 2012, ICANN launched the new gTLD program, which aimed to provide greater flexibility for registrants to create unique and innovative website names. This initiative also alleviated the overcrowding in the legacy gTLD market, offering more options for domain registration. Since the program's introduction, over a thousand new gTLDs have been delegated to the root zone, significantly expanding the domain name landscape.

DNS Record. DNS records are fundamental components of the Domain Name System (DNS), serving as mappings that enable domain names to link to specific internet resources, such as IP addresses, email servers, and authoritative name servers. Each DNS record type provides unique information and functionality essential for domain operation. For instance, `A` records (Address records) link a domain to an IPv4 address, directing users to the correct server when they access a website. `NS` records (Name Server records) specify which servers are authoritative for a domain, manage DNS queries, and ensure accurate routing.

DNS records may differ depending on the geographic or network location, known as the vantage points, from which the DNS query is made. This variation occurs because DNS configurations can be adapted to present different responses based on the requester's location, such as content delivery optimization or load balancing.

2.2 Phishing Attack and Tactic

Phishing attacks are a type of advanced social engineering where cybercriminals deceive victims into divulging sensitive information. Phishing attackers craft fake websites that closely resemble legitimate ones (*e.g.*, Facebook or PayPal), deceiving victims into entering their credentials.

Phishing Tactics for Domain Registration. The choice of the registrar and TLD can significantly impact a domain's visibility, cost, and accessibility, with certain TLDs (*e.g.*, `.tk` or `.xyz`) often being cheaper or subject to less stringent registration requirements. Phishing attackers frequently take advantage of this aspect of domain registration, choosing low-cost or lenient TLDs to host their malicious sites in large numbers while minimizing expenses [46]. Additionally, some registrars (*e.g.*, `Alibaba Cloud` [12]) have minimal verification protocols, making it easier for attackers to quickly register multiple domains in bulk under anonymous or fabricated identities [5]. This practice allows attackers to operate on a large scale, using each domain temporarily until it is flagged or blocked by detection systems, then transitioning to newly registered domains.

Phishing Tactics for Domain Name. When conducting phishing attacks, attackers employ various domain registration strategies to deceive users. They commonly use typosquatting, registering domains with subtle misspellings, such as `paypaI.com` (using a capital `I` instead of `L`) or missing letters such as `goole.com`. Another tactic involves creating domain variations by adding words or modifying the structure, resulting in domains like `paypal-secure-login.com` or `login-paypal.net`. Attackers also abuse different top-level domains (TLDs), using alternatives like `.co` or country-specific codes instead of the legitimate `.com`.

3 Problem Statement

Phishing remains a major security threat, with traditional blocklist-based defenses (*e.g.*, Google Safe Browsing—Google Chrome default anti-phishing system) suffering from significant detection delays. These systems often take hours or days to update after new phishing domains are registered, creating a critical window of vulnerability during which attackers can successfully target victims [40–43, 48, 49].

Addressing phishing at the DNS level—when domains are first registered—is crucial, as domains are the primary gateway to phishing websites. However, while previous studies [28, 44, 46, 48, 49, 51] have focused on URL patterns, visual content, and blocklist data, there is limited understanding of how attackers exploit DNS registration strategies for phishing attacks. To this end, our work aims to bridge this knowledge gap by focusing on maliciously registered domains for phishing attacks and their abuse of DNS systems. Particularly, we seek to answer our research questions through our analysis using our dataset of phishing domains: **RQ1:** *What are the characteristics of maliciously registered domains, and how can we find maliciously registered domains?* and **RQ2:** *What is the lifecycle of a maliciously registered domain?*.

Table 1: Overview of Our Collected Dataset from July 2021 to October 2024 (39 months). We collect a total of 2.3M phishing URLs and 765K domains.

Type	# URLs	# Domains	# TLD
APWG [6]	2,184,835	697,237	1,203
phishunt.io [56]	262,755	66,743	598
PhishStats [54]	221,331	57,299	541
OpenPhish [52]	115,804	26,127	480
Malware-filter [14]	76,465	24,300	470
PhishTank [55]	5,579	1,695	195
Phishing.Database [45]	393	236	51
Total (Distinct)	2,294,267	765,910	1,258

– APWG: collected from Jul. 15, 2021 to Oct. 31, 2024.
– Others: collected from May 31, 2024 to Oct. 31, 2024.

4 Dataset Collection

To address our research questions, we collect a dataset comprising phishing URLs (Section 4.1), DNS records using a custom-built crawler (Section 4.2), and registration timestamps of phishing domains to analyze their characteristics and lifespans (Section 4.3).

4.1 Phishing URL and Domain Collection

As shown in Table 1, we first collect 2.3M phishing URLs and their associated 765K distinct domains (1,258 TLDs) across a 39-month period spanning July 2021 to October 2024 from multiple prominent phishing blocklists including APWG (Anti-Phishing Working Group) [6], Malware-filter [14], OpenPhish [52], Phishing-Database [45], phishunt.io [56], PhishStats [54], and PhishTank [55]. These sources have been used to better understand the phishing ecosystem [36, 39, 48–51]. Particularly, APWG is a global industry association of anti-phishing entities, including banks and financial services companies, Internet service providers, law enforcement agencies, and security vendors. APWG maintains an extensive database of phishing URLs gathered from multiple sources.

4.2 DNS Record Collection

To answer our research question (**RQ1:** *What are the characteristics of maliciously registered domains, and how can we find maliciously registered domains?*), we develop a comprehensive DNS data collection system to monitor and analyze how phishing attackers configure and modify their DNS settings across different geographic locations. Our system periodically collects DNS records types of our collected phishing domains (*i.e.*, `A`, `AAAA`, `NS`, `MX`, `TXT`) to provide detailed insights into their behavior.

DNS Crawler Design. Figure 1 illustrates our data collection process. We implement a multi-threaded crawler designed for scalability and reliability, using concurrent processing to efficiently handle thousands of domain queries. The crawler maintains a connection pool for database access and implements file-locking mechanisms to prevent data corruption during parallel operations. The crawler collects detailed DNS information using the `dig` command with comprehensive parameters. This approach enables the recursive collection of DNS records, capturing all possible types. For reliability, our system implements a retry mechanism with exponential backoff, attempting each query up to 5 times before marking it as failed.

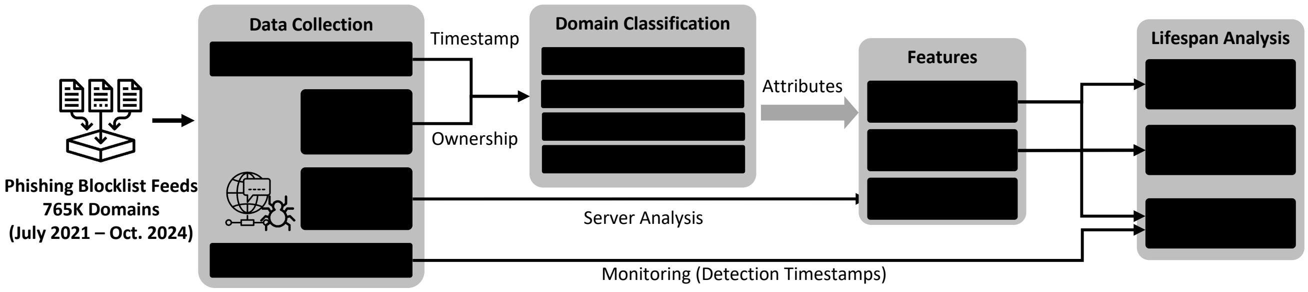


Figure 1: Overview of Our DNS Analysis on Phishing Domains.

Our crawler operates at 30-minute intervals, enabling us to capture both gradual changes and modifications in DNS configurations. This high-frequency polling is crucial for detecting dynamic DNS behaviors that phishing attackers might employ to evade detection, such as fast-flux DNS or rapid record updates. The system stores DNS responses in a structured JSON format, organized by domain, timestamp, and vantage point.

Our data collection period spanned from June 6, 2024, to October 31, 2024. We gathered URLs from blocklist feeds and extracted their domains and subdomains to perform DNS queries during this period. Using our crawler, we collected a total of 94,798 domains, including subdomains, with 11,932 being unique domains.

Vantage Points. Moreover, to detect location-based DNS configurations, we query DNS records from 10 geographically diverse DNS resolvers. These include global providers (Google, Cloudflare, Quad9, OpenDNS) and regional servers across six continents (Brazil, South Africa, UK, Australia, South Korea, US). This distributed approach reveals if phishing domains serve different DNS responses based on geographic location—a technique attackers might use to evade detection or target specific regions.

4.3 Domain Registration Collection

To investigate the lifecycle of maliciously registered domains (**RQ2:** "*What is the lifecycle of a maliciously registered domain?*"), we collect registration information (including timestamps and registrars) of our collected phishing domains. We first utilize WHOIS and the Registration Data Access Protocol (RDAP) [57] from registrars and registries as WHOIS and RDAP provides basic information, such as registrar names and domain registration/expiration dates.

GDPR Restriction. However, due to the European General Data Protection Regulation (GDPR), the registration timestamp and the registrant's information (such as their name, address, and phone number) can be unavailable to the public. To this end, we leverage the methodology of COMAR [44] to obtain registration timestamps of the domains whose information is hidden. Furthermore, we also utilize DNS Zone files from DNS Coffee [66] and DZDB [10] for more comprehensive registration timing analysis. These services daily collect and archive TLD Zone files from ICANN [29]. The Zone file data provides first-appearance and last-seen timestamps of domains; the last-seen timestamp indicates when a domain has been deregistered and is no longer active. We also utilize passive DNS (pDNS) data through DomainTools' Farsight DNSDB [17]. This dataset includes a first-seen timestamp, indicating the earliest recorded observation of a domain in the passive DNS.

Our Collected Registration Data. Our dataset includes domain registration timestamps collected from various sources: WHOIS (25,987 domains), RDAP (436,176 domains), CT logs (71,156 domains), DomainTools (27,929 domains), and DNS Coffee (526,867 domains, inclusive of DZDB data). In total, we have 526,954 registration timestamps for unique domains. In sum, our approach enables us to achieve 76.3% (526,954 out of 690,502) coverage of our collected domains. While relying solely on registration timestamps from WHOIS and RDAP provides 62.4% (431,011 domains) coverage, incorporating additional data sources such as zone files, pDNS data, and CT logs significantly improves the completeness of our timestamp data.

5 Identifying Maliciously Registered Domains

We first define maliciously-registered domains and then devise a method to identify the ones for phishing attacks. We further analyze the bulk registrations of phishing domains.

Def. of Maliciously-registered Domains. Phishing domains can be classified into two categories: maliciously registered domains and compromised domains. A maliciously registered domain is intentionally purchased by an attacker for malicious purposes. In contrast, a compromised domain is a legitimate domain originally used for benign purposes, but attackers exploit vulnerabilities of web servers and inject malicious content (*e.g.*, phishing pages) into the benign servers. Detecting maliciously registered domains at an early stage is a critical step in preventing phishing attacks effectively.

Identification of Maliciously-registered Domains. We utilize Tranco 1M domains [64] as a reference to filter out both legitimate domains and web hosting (or website builder) service domains from our collected phishing domains. For example, while '`blogspot.com`' is a legitimate blogging service, attackers may create subdomains, such as '`usps-tracking-service.blogspot.com`' for phishing purposes. After removing the platform-based phishing domains, our list remains 689,492 domains.

Furthermore, we leverage the previous approaches [11, 16, 27, 32, 44] on finding maliciously registered domains. Especially, COMAR [63] demonstrated a 95% accuracy using lexical features and registration timestamps in domains. The method from COMAR includes nine lexical features (*i.e.*, presence of a brand name in the domain name, path part of URL, and misspelled target brand name in the domain name). By merging those features and additional features we discovered, we design our method to detect maliciously registered domains by using the following four steps: (1) brand

Table 2: Maliciously-registered Domain. Each steps are taken after removing the Tranco Top 1M [64] list of domains (total of 689,492).

Type	# of URLs	# of Domains*
(1) Brand Name in Domain	709,694	247,699 (35.9%)
(2) Squatted Domain	472,320	180,468 (26.2%)
(3) Random-looking Domain	283,366	194,099 (28.2%)
(4) Bulk-registered Domain	69,599	54,787 (7.9%)
Mal. Total†	1,406,525	455,525 (66.1%)

*: Due to the overlap, total domains are over 100%

name in domains, (2) squatted domains, (3) random-looking algorithmic domains, and (4) bulk registered domains. As shown in Table 2, each steps are taken after removing the Tranco 1M [64] domains from the total list of domains.

(1) Brand Name in Domain. The first approach to identifying maliciously registered domains involves detecting brand names within the domain or subdomain (*e.g.*, `usps-security.example.com`, or `www.usps-security-login.com`). To establish a comprehensive baseline, we curate a list of the top 1,000 most targeted brands in our collected datasets (*i.e.*, APWG), covering 97% of the domains in our dataset. Domains or subdomains containing any of these brand names are flagged as part of this category. Our analysis reveals that 33.9% of domains in the dataset incorporate brand names in their domain or subdomain, highlighting the prevalence of this tactic among phishing attackers. Detailed results for maliciously registered domains across all categories are summarized in Table 2.

(2) Squatted Domain. The second category is one of the most common tactics used by phishing attackers: exploiting squatted domains. These domains incorporate a modified version of a brand name in the domain or subdomain, closely mimicking legitimate brand domains to deceive users. For example, a phishing website targeting `facebook.com` might use a squatted domain such as `faceb{o}ook.com` to trick victims into believing they are accessing an authentic website.

To identify potential squatted domains, we employ the dnstwist tool [19], which generates domain name variations using various squatting techniques and widely used in previous works [25, 35, 61, 63]. We apply this tool to the top 200 most targeted brand names, which account for 90% of the domains in our dataset. This process generates 765,444 possible squatted domains based on techniques such as adding extra characters to the domain name (*e.g.*, `facebook0.com` from `facebook.com`), modifying a single bit in the domain name (*e.g.*, `faaebook.com`), replacing characters with visually similar alternatives (*e.g.*, `faceb0ok.com`, where `o` is replaced with the number, `0`), and adding hyphens or extra prefixes (*e.g.*, `face-book.com` or `dfacebook.com`). Our analysis shows that 26.2% of domains in our dataset are squatted domains.

(3) Random-looking Algorithmic Domain. The random appearance of algorithmically generated domains makes them hard to detect [20, 58]. Attackers exploit this trend by capitalizing on users' tendencies not to scrutinize domain names closely before clicking on links, even when the domain looks suspicious. To find random-looking algorithmic domains, we follow the approach in [58] by matching domains with English word lists. We use [60], a word list containing 108,687 words, to identify domains that include any

Table 3: Top 10 Registrar in Bulk Registered Domains. `Alibaba` stands out as the registrar associated with the highest number of bulk-registered domains.

Rank	Registrar	# of Domains	Country
1	ALIBABA SGP.* [12]	4,180 (7.6%)	CN
2	Alibaba (Wanwang)† [5]	2,599 (4.7%)	CN
3	SAV.COM [59]	2,093 (3.8%)	US
4	GoDaddy.com [23]	1,845 (3.4%)	US
5	Gname.com Pte. [22]	1,560 (2.8%)	SGP
6	Alibaba Cloud‡ [12]	1,352 (2.5%)	CN
7	NameSilo [47]	1,285 (2.3%)	US
8	Network Solutions [62]	623 (1.1%)	US
9	Dynadot Inc [18]	618 (1.1%)	US
10	Aceville Pte. [2]	604 (1.1%)	SGP
Total		54,787 (100%)	-

*: ALIBABA.COM SINGAPORE E-COMMERCE PRIVATE
†: Alibaba Cloud Computing Co., Ltd. (Wanwang)
‡: Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn)

English words. We apply this process after removing the brand in the domain and squatted domains, leaving a total of 194,099 domains.

As shown in Table 2, a significant portion of domains (28.2%) are random-looking algorithmic domains. While such domains may appear suspicious to a human [58], automated detection tools often struggle to classify them as malicious due to their lack of clear patterns or recognizable features.

(4) Bulk Registration of Domain. Attackers often register many malicious domains simultaneously through bulk registration to maximize profits with minimal effort [28]. A phishing campaign can involve registering multiple domains at the same time and deploying multiple webpages with different domains. Even if one domain is blocklisted, an attacker can rely on others to continue the attack. Our method to find bulk registered domains includes three conditions that must all be met: registered at the same time, registered through the same registrar, and domain names are similar (using Levenshtein distance [37]).

Bulk-registered domains, often created simultaneously through the same registrar, account for 7.9% of the domains in our dataset, as shown in Table 3. While this percentage represents a smaller subset of the dataset, it carries significant implications.

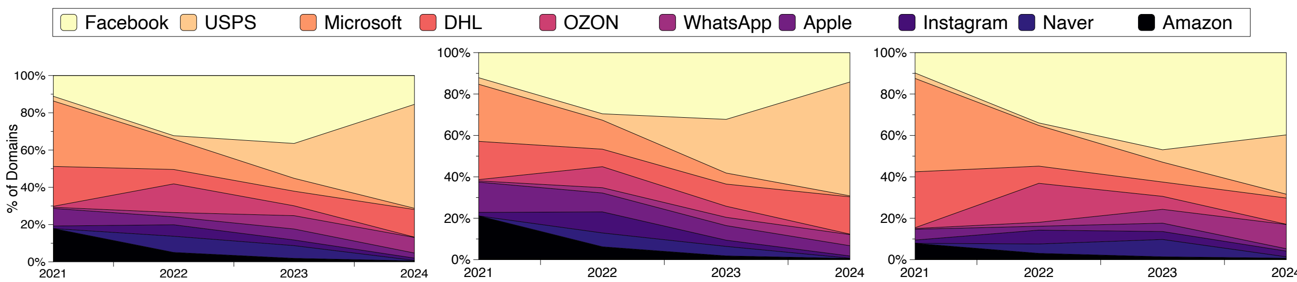
Notably, `Alibaba Cloud`[12] frequently serves as a registrar for these domains, offering bulk registration services[4]. Furthermore, it actively promotes bulk registrations through discounted pricing [5], as illustrated in Appendix A.This combination of bulk registration functionality and discounted pricing likely lowers the barrier for registering multiple domains, making it an attractive option for attackers. This practice enables attackers to sustain their operations by registering multiple domains in bulk, ensuring that some remain active even after others are detected. Some registrars adopt proactive measures, such as stricter verification or limits on bulk purchases, which significantly reduce the malicious use of bulk-registered domains.

Manual Validation. We randomly select 1,000 domains from our identified maliciously registered domains. Then, we manually validate our method of identifying maliciously registered domains by examining the contents of the phishing domains. Specifically,

Table 4: Top 10 Targeted Brands. Popular brands (*e.g.*, USPS, OZON, Instagram) predominantly utilize .top, .tk, .ml than the origin of its brand (*e.g.*, .com, .ru).

Brand	Country	Total	Malicious Domains	Compromised Domains	Malicious Domains			Compromised Domains		
					TLD*	TLD Count	Unique§	TLD*	TLD Count	Unique§
Facebook	US	66,700	38,817 (58.2%)	27,227 (40.8%)	.com	11,485 (29.6%)	439	.com	10,764 (39.5%)	324
USPS	US	41,691	37,533 (90.0%)	4,109 (9.9%)	**.top**	15,489 (41.3%)	259	**.top**	1,835 (44.7%)	153
Microsoft	US	26,717	13,681 (51.2%)	12,438 (46.6%)	.com	5,759 (42.1%)	449	.com	6,358 (51.1%)	371
DHL	GER†	23,539	15,784 (67.1%)	7,277 (30.9%)	.com	5,741 (36.4%)	451	.com	3,612 (49.6%)	322
OZON	RUS†	18,513	10,248 (55.4%)	8,465 (45.7%)	**.tk**	4,549 (44.4%)	34	**.tk**	4,600 (54.3%)	17
WhatsApp	US	11,521	8,264 (71.7%)	3,163 (27.5%)	.com	2,363 (28.6%)	162	.com	1,198 (37.9%)	104
Apple	US	11,253	8,942 (79.5%)	2,056 (18.3%)	.com	3,385 (37.9%)	234	.com	918 (44.6%)	138
Instagram	US	11,181	7,337 (65.6%)	3,681 (32.9%)	**.ml**	1,482 (20.2%)	212	.com	982 (26.7%)	165
Naver	KOR†	11,030	7,207 (65.3%)	3,725 (33.8%)	.com	2,506 (34.8%)	269	.com	1,549 (41.6%)	195
Amazon	US	9,473	7,390 (78.0%)	2,000 (21.1%)	.com	2,086 (28.2%)	192	.com	996 (49.8%)	110

*: Most common TLD in brands. §: # of unique TLD in brand. †: GER: Germany, RUS: Russia, KOR: Korea.



(a) Top 10 Brand by Year All. **(b) Top 10 Brand by Year (Malicious).** **(c) Top 10 Brand by Year (Comp.).**

Figure 2: Top 10 Brand by Year. USPS increases dramatically from 2022 to 2024, specifically in maliciously registered domains. On the other hand, Microsoft decreases in all domains, DHL increases in maliciously registered domains but decreases in the compromised domains.

we utilize historical data from the Wayback Machine [7] to identify domains that either lack historical snapshots or display content designed to mimic legitimate webpages.

Our analysis reveals that 72.3% of the examined domains do not have any historical data in the Wayback Machine. Among the remaining 27.7%, 14.8% domains redirect to error pages, while the remaining 12.9% of domains host malicious content pages.

Takeaway: We combined the existing method with our new method of identifying maliciously registered domains. Maliciously registered domains are over half of phishing domains (66.1%). Phishing attackers often exploit bulk registration services, such as those offered by `Alibaba Cloud`. Notably, among registrars that provide bulk registration, `Alibaba` emerges as the most frequently abused platform for registering domains in bulk.

6 Characteristics of Maliciously registered Domains

We analyze DNS components of maliciously registered domains, including their targeted brands, TLDs, and DNS records, to gain insights into their characteristics.

6.1 Targeted Brand

We utilize target brand information from the APWG dataset. In our analysis, we identify a diverse range of targeted brands, with `Facebook` standing out as the most targeted brand, followed by `USPS` as shown in Table 4. These two brands alone account for a significant portion with 15.5% (108,391 out of 697,237) of phishing domains, reflecting their widespread recognition and trust among users.

As shown in Figure 2, a clear trend emerges among popular targeted brands. Notably, `USPS` is the second most targeted brand, accounting for 6.0% of phishing domains. Interestingly, while `USPS`-targeted domains were minimal in 2021 and 2022, there has been a dramatic increase since 2023. This finding aligns with previous reports on phishing domain trends [32]. Conversely, `Microsoft` shows an overall decline in targeting, with a more pronounced decrease observed in compromised domains, as illustrated in Figure 2(c). Additionally, `DHL`-targeted domains demonstrate an increasing trend in maliciously registered domains over the years, while showing a decline in compromised domains.

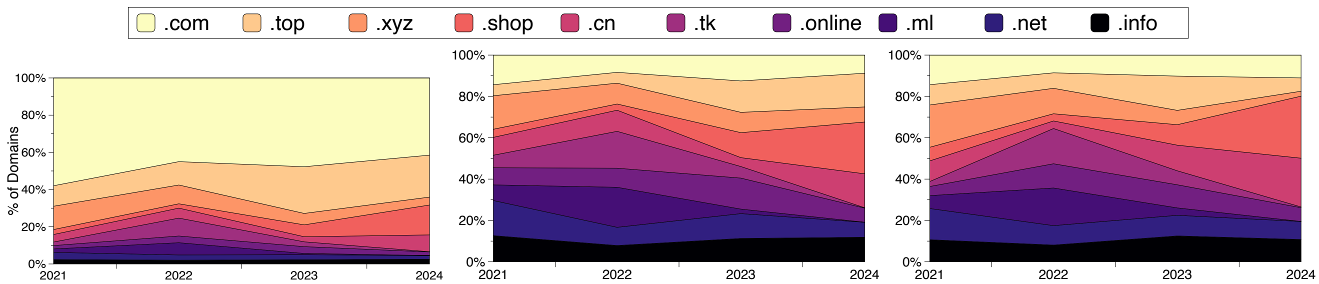
6.2 Top-level domain (TLD)

We investigate the use of TLDs in phishing domains and assess whether certain TLDs are disproportionately abused. Our analysis

Table 5: Top 10 TLDs by Year. New-gTLD with lower registration costs is widely used in maliciously registered (.top, .xyz, .shop, .online) than compromised domains (.net, .info). Freenom usage decreases and (*e.g.*, .cn increased in 2024 where .tk and .ml decreased)

TLD	Total	Maliciously Registered Domains					Compromised Domains					Price (USD)*	Types†	Freenom
		2021	2022	2023	2024	Total	2021	2022	2023	2024	Total			
.com	218,267	19,359	53,795	42,376	26,949	142,479	10,837	30,051	20,813	14,087	75,788	$6	gTLD	No
.top	84,686	2,735	12,792	19,519	18,968	54,014	3,005	10,612	13,721	3,334	30,672	**$1**	new gTLD	No
.xyz	37,698	3,545	10,520	5,396	3,624	23,085	2,985	8,310	2,732	586	14,613	**$1**	new gTLD	No
.shop	30,065	764	2,790	5,905	11,081	20,540	628	1,532	2,550	4,815	9,525	**$1**	new gTLD	No
.cn	24,708	1,639	9,234	2,045	7,060	**19,978**	471	798	1,582	1,879	**4,730**	$5	ccTLD	No
.tk	22,453	779	10,931	1,802	**52**	13,564	213	7,001	1,623	**52**	8,889	$7	ccTLD	**Yes**
.online	14,409	679	3,609	3,084	1,271	8,643	254	3,123	1,741	648	5,766	**$1**	new gTLD	No
.ml	14,154	726	8,868	526	**5**	10,125	251	3,388	390	**0**	4,029	$12	ccTLD	**Yes**
.net	12,672	1,302	3,217	2,309	1,260	8,088	691	1,987	1,233	673	4,584	$10	gTLD	No
.info	10,619	974	2,891	2,182	2,076	8,123	266	934	843	453	2,496	$2	gTLD	No

*: Cost to register a domain in each TLD [63]. †: gTLD vs. ccTLD. Note that years 2021 and 2024 are not 12 months.



(a) Top 10 TLD by Year All.

(b) Top 10 TLD by Year (Malicious).

(c) Top 10 TLD by Year (Comp.).

Figure 3: Top 10 TLD by Year. While .com is the most used, .shop, .cn increase over the years.

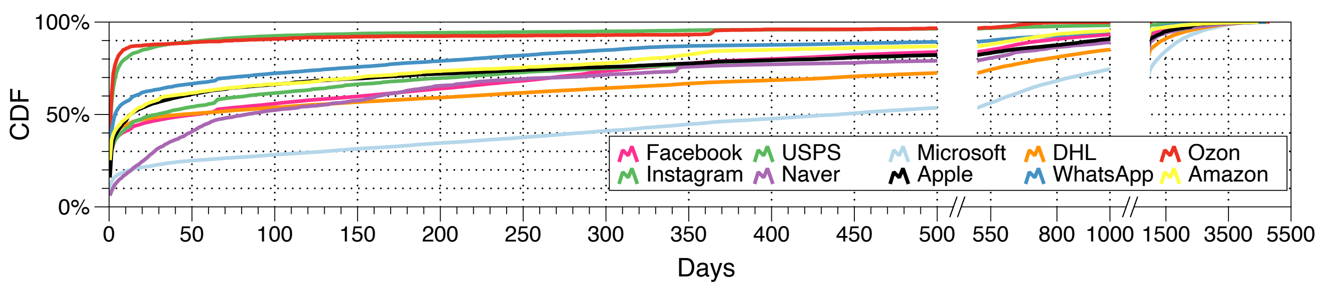


Figure 4: Days Between Registration and Detection by Top 10 Brand.

considers the varying registration costs across TLDs, which may influence attackers' choices and strategies.

Motivation. TLD choice plays a significant role in domain registration for phishing attacks. Attackers may opt for cheaper TLDs to minimize costs or strategically use the same TLD as the targeted brand to enhance impersonation (*e.g.*, using .com for brands that also use .com). According to a phishing report [32], Freenom TLDs were among the most commonly exploited by phishing attackers, as they offered free registrations. However, after reports revealed widespread abuse of this functionality for malicious domain registration, Freenom ceased offering free registrations in early 2023. Moreover, a subsequent report by Interisle [32] noted a shift, with phishing domains in ccTLDs increasing after Freenom's policy change. To examine whether our findings align with this trend, we analyze TLD usage in phishing domains, focusing specifically on maliciously registered domains to uncover patterns and their implications.

Result: Trend of TLD. Table 5 highlights significant trends in TLD usage across phishing domains, illustrating attackers' preferences and the influence of policy changes. The .com TLD dominates the landscape with 218,267 (31.3% out of 697,237) total phishing domains, likely due to its credibility and widespread familiarity, which enhance its effectiveness for deception. Low-cost new gTLDs, such as .top and .shop, become prominent in our result, with 84,686 (12.1%) and 37,698 (5.4%) domains, respectively, reflecting attackers' preference for inexpensive and lenient TLDs. As shown in Table 5, the lower registration costs of new gTLDs (with prices as low as $1 in our dataset) may contribute to their increased exploitation by phishing domains.

Freenom TLDs (*e.g.*, `.tk`) are heavily exploited in earlier years, but seen a dramatic decline, dropping from 10,931 domains in 2022 to merely 52 domains in 2024, after Freenom discontinued free registrations in 2023. This finding aligns with a previous report [32]. Additionally, as shown in Figure 3, the growing presence of `.cn`, from 764 in 2021 to 7,060 in 2024 domains, signals a strategic adaptation by attackers to target TLDs with potentially weaker enforcement mechanisms [32].

As illustrated in Figure 3, there is a notable increasing trend in the use of new gTLDs, particularly `.top` and `.shop`. Interestingly, the use of `.top` in maliciously registered domains has steadily increased over the years, while its usage in compromised domains shows a decline in 2024. In contrast, `.shop` demonstrates a consistent increase in usage across both maliciously registered and compromised domains.

Takeaway: Phishing domains often exploit new gTLDs due to their lower registration costs. Notably, when `Freenom` discontinued offering free domain registrations, the usage of `.cn` domains increased concurrently. Certain new gTLDs, such as `.shop`, exhibit distinct trends between maliciously registered domains and compromised domains, highlighting different attack strategies.

Using Different TLD than Original Brand Domain. Phishing domains do not always use the same TLD as their original domains. For instance, phishing attackers often register `Facebook`-targeted domains using alternative TLDs such as `.top`, rather than `.com` that used by `Facebook`. Similarly, `USPS`, the second popular targeted brand in our analysis, is frequently targeted using `.top` domains instead of the brand's original `.com`. Another example is `OZON`, ranked as the 5th most targeted brand, with 49.42% of its phishing domains registered under the `.tk` instead of its original `.ru`. Both `.top` and `.tk` are significantly cheaper than `.com` for registration, with `.tk` previously offered for free by Freenom until January 2023. Interestingly, both targeted brands `USPS` and `OZON` have the quickest detected time by blocklists as shown in Figure 4. We will discuss detection time across different brands in Section 7.1.

Another noteworthy observation from Table 4 is that 44.39% of `OZON`-targeted domains are registered under `.tk`, which is significantly more popular than any other brand. Additionally, `OZON`-targeted domains exhibit the smallest number of unique TLDs (34) among the top 10 brands. Furthermore, as shown in Figure 2, `OZON` demonstrates a decline in phishing activity over time. These findings suggest that attackers targeting `OZON` often prefer low-cost TLDs, such as those offered by Freenom, to minimize costs and maximize the scalability of their phishing campaigns.

Takeaway: Phishing attackers prefer low-cost TLDs like `.top` and `.tk` to target brands such as `USPS` and `OZON`, with `OZON` relying on `.tk` for 44.39% of its phishing domains. These brands also show the fastest detection times by blocklists, highlighting the importance of monitoring cost-effective TLDs to combat phishing campaigns.

Maliciously-registered Vs. Compromised. The comparison between maliciously registered and compromised domains reveals notable differences in their TLD preferences. Among a total of 218,267 `.com` domains, 142,479 (65.3%) were maliciously registered, while 75,788 (34.7%) were compromised, indicating that attackers leveraging `.com` domains often register them intentionally for malicious purposes. Conversely, new gTLDs such as `.top` and `.xyz` also show a strong preference for malicious registrations, with 54,014 (63.8%) and 23,085 (61.2%) domains, respectively, highlighting attackers' exploitation of low-cost TLDs for scalability. In contrast, Freenom TLDs like `.tk` saw relatively balanced usage between maliciously registered and compromised domains before policy changes restricted their availability. These patterns suggest that maliciously registered domains favor low-cost or lenient TLDs, while compromised domains may be distributed across a broader range of TLDs, reflecting their opportunistic use of existing infrastructures. This distinction underscores the importance of targeted monitoring and stricter enforcement in TLDs that are disproportionately used for malicious registrations.

We analyze the targeted brands between maliciously registered domains and compromised domains. `Facebook` is the most used targeted brand, with 66,700 phishing domains, of which 58.20% are maliciously registered. `USPS` and `Microsoft` follow, with 41,691 and 26,717 domains, respectively. `USPS` exhibits an exceptionally high proportion of maliciously registered domains (90.03%), indicating that attackers targeting this brand prefer creating new domains rather than compromising existing ones. Microsoft demonstrates a more balanced split, with 51.21% malicious registrations and 46.55% compromised domains, suggesting a dual approach in leveraging both new and existing infrastructures.

Takeaway: New gTLDs (*e.g.*, `.top`, `.xyz`) are more prevalent in maliciously registered domains, while compromised domains favor legacy gTLDs (*e.g.*, `.net`, `.info`). Freenom TLDs like `.tk` and `.ml` have declined, while `.cn` has increased in 2024.

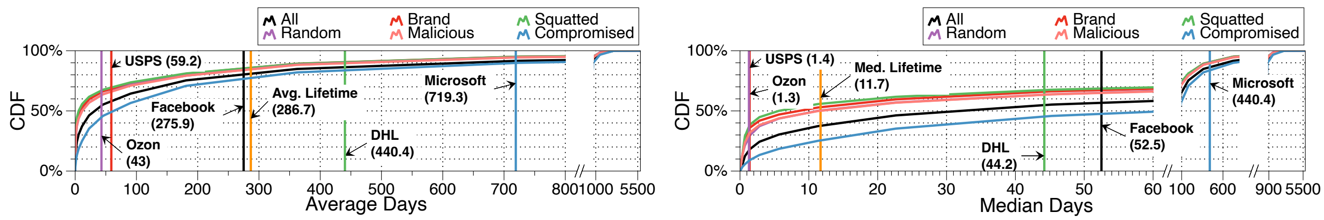
6.3 DNS Records

We characterize the DNS records of maliciously registered domains collected by our DNS crawler.

DNS Records. We study the values of commonly used DNS record types (*e.g.*, `A`, `AAAA`, `CNAME`, `NS`, `MX`, and `TXT`). Phishing attackers often configure DNS records to evade detection, frequently altering them using techniques such as fast-flux DNS. Our analysis reveals that 21.4% of domains exhibit record changes, with an average frequency of 79.4 days and a median of 125.2 days.

We study the types of DNS records configured in phishing domains. `NS` records were the most common, with a total of 51,459, followed by `A` records (13,218), `SOA` records (8,960), and `TXT` records (5,573). Focusing specifically on maliciously registered domains, we specifically examined those that exhibited DNS record changes. Our analysis shows that only 4.6% of these domains (117 out of 2,550) demonstrated record changes over time. This suggests that modifying DNS records is not a commonly used tactic among maliciously registered phishing domains.

To understand the scenarios behind DNS record changes, we manually reviewed domains that exhibited such changes over time. One common case involved NS record changes, where domains shifted from one DNS provider to another (*e.g.*, from Cloudflare to Google). Such changes are often motivated by the desire to leverage specific services offered by different DNS providers. For instance,



(a) Average Delays (days) Between Registration and Detection. **(b) Median Delays (days) Between Registration and Detection.**

Figure 5: Delays (days) Between Registration and Detection. Vertical bars show average (or median) days between registration time and detection time of the top 5 most targeted brands.

attackers may switch to providers like Cloudflare to utilize features, such as free SSL certificates, which are available for a limited duration [13].

Our analysis reveals that phishing domains show a strong preference for hosting on Amazon Web Services (AWS) infrastructure. Specifically, we extract all IP addresses associated with `A` records and utilize the `Summarize IP` feature provided by IPinfo [34] to gain insights into their hosting characteristics. Among the Autonomous System Numbers (ASNs) analyzed, AS16509 (Amazon.com, Inc.), a primary ASN for AWS, hosts 81.2% of the phishing domains, while an additional 15.4% are hosted on AS14618 (Amazon.com, Inc.), another AWS-associated ASN. Combined, these two ASNs account for 96.6% of all analyzed phishing domains, indicating a significant reliance on AWS services. This preference may be attributed to AWS's scalability, cost-effectiveness, and global reach, which make it an attractive option for attackers to host phishing domains. In comparison, other hosting providers, such as Google LLC (1.5%), JSC Selectel (0.2%), and DigitalOcean, LLC (0.1%), host far fewer phishing domains.

Vantage Point of DNS Server. Phishing attackers can configure location-aware DNS responses. This allows attackers to deliver localized phishing content (*e.g.*, Spanish-language phishing pages for victims in South America) or to evade detection by serving benign pages when accessed from certain locations commonly used by detection systems.

Our preliminary analysis shows that some phishing domains adapt their content to different languages based on the location of the user accessing them. However, we do not find any evidence that these phishing domains alter their DNS records based on the vantage point of the queried DNS servers. Instead, further investigation reveals that these domains implement language customization through client-side code rather than DNS configuration.

TTL in DNS Records. In DNS records, the time-to-live (TTL) specifies how long DNS settings are cached before they are automatically refreshed. Typical TTL values are 12 or 24 hours, with recommended minimum and maximum values of 1 hour (3600 seconds) and 24 hours (86400 seconds), respectively [33]. 2.1% of the domains use TTL values less than 60 seconds, and 25.8% use values shorter than 1 hour (3600 seconds) from our dataset. Only 2.9% of the domains set TTLs longer than 12 hours, and among those, 31 domains set values between 12 and 24 hours. The median TTL value across domains is 3,994 seconds, while the average is significantly higher at 60,827 seconds. The use of short-lived TTLs can facilitate fast-flux DNS, a technique that frequently changes IP addresses to evade detection [9, 21] and often employ by attackers [15].

> **Takeaway:** Our analysis finds that 21.4% of domains change their DNS records frequently. 2.1% of phishing domains configure their DNS TTL values to less than 60 seconds, a configuration commonly associated with fast-flux DNS techniques.

7 Lifespan of Phishing Domains

This section examines the lifecycle of phishing domains, focusing on two critical phases: (1) the time from registration to detection, (2) the time from detection to deactivation, and (3) the comparison of detection time between blocklists. These phases provide insights into how phishing attackers sustain their domains to maximize monetization and evade timely countermeasures. By analyzing detection delays and post-detection persistence across different domain types, brands, and registration strategies, we uncover characteristics in the lifespan of phishing domains (*i.e.*, maliciously registered). Our findings highlight the need for improved detection mechanisms to reduce delays and more robust enforcement measures to ensure rapid domain takedown, thereby limiting attackers' ability to exploit these domains.

7.1 Time Taken between Registration to Detection (Detection Delay)

In this section, we analyze how phishing domains are detected by blocklist after registration.

Motivation. Maliciously registered domains can be blocked in advance when compared to compromised domains. Phishing domains exhibit significant variation in the time it takes to be detected after registration, influenced by the type of domain and the targeted brand. As shown in Figure 5, these differences highlight both quicker detection for some brands and prolonged delays for others.

Result: Overview of Detection Delay. Across all domains, the overall median detection time is 42.4 days, with an average of 286.2 days. For the top 10 most targeted brands, the detection times have a slight improvement over these values, with an average of 286.2 days and a significantly shorter median of 11.7 days. This suggests that well-known brands tend to benefit from quicker median detection times compared to less prominent brands, likely due to more active monitoring and stronger anti-phishing measures.

Detection Time between Targeted Brands. `USPS` (United States Postal Service) [65], a U.S. federal agency providing postal services,

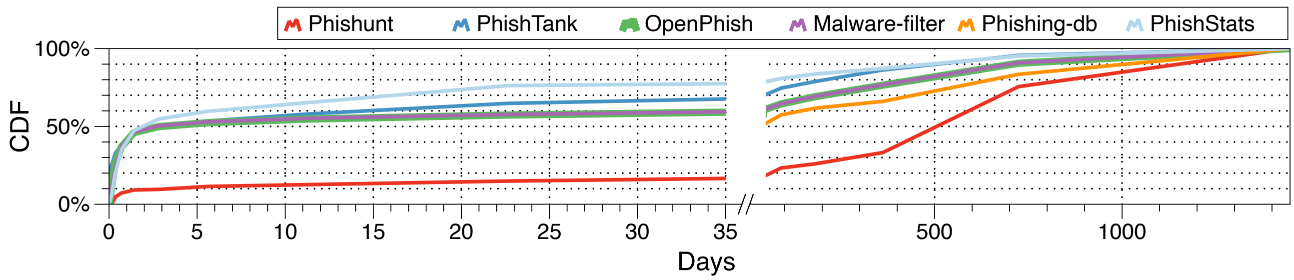


Figure 6: Days Between APWG Detection and Other Blocklists. Other than Phishunt, all 5 blocklists show similar median delays (2.3 to 4.4 days except the Phishunt).

and OZON [53], a Russian e-commerce platform founded in 1998, stand out with the fastest average detection times among targeted brands. USPS has a median of 1.4 days (average of 59 days), and OZON has a median of 1.3 days (average of 42.9 days). These quicker detections may result from more active monitoring systems or simpler phishing tactics that are easier to identify.

Both brands are targeted using non-original TLDs (Section 6.2), which are often cheaper to register. Also, the detection as shown in Figure 4, detection time of USPS and OZON is quickest with a median of 1.4 days and 1.3 days respectively. Some registrars, such as Freenom, provide APIs for the immediate takedown of phishing domains upon detecting signs of abuse [3]. This suggests that attackers' choice of cost-effective TLDs may have inadvertently backfired, as these domains could be removed quickly.

Domains targeting Microsoft take the longest to be detected, with an average detection time of 719 days (median of 440.4 days). Facebook, despite being the most impersonated brand, has a moderate detection time of 275 days (median of 52.5 days). These findings highlight significant disparities in detection efficiency across brands and TLDs, emphasizing the impact of attackers' TLD choices on detection timelines.

Maliciously-registered Vs. Compromised. As shown in Figure 5, the detection times vary across different categories of maliciously registered domains. Overall, compromised domains consistently have slower detection times compared to maliciously registered domains, though the difference is not substantial. Specifically, the median detection time for maliciously registered domains is 16.3 days, with an average of 206.4 days, while compromised domains have a median detection time of 86 days and an average of 332.1 days. This indicates that current detection methods do not perform significantly better at identifying maliciously registered domains compared to compromised domains. We will discuss potential future directions in Section 8.

Takeaway: Detection delays for phishing domains vary, with maliciously registered domains detected faster (median 16.3 days) than compromised ones (median 86 days). Brands like USPS and OZON see rapid detection (medians of 1.4 and 1.3 days), while others, like Microsoft, face significant delays (median 440.4 days and 52.5 days, respectively).

7.2 Time Taken between Registration and Deregistration (Takedown Delay)

Figure 7 highlights the significant variation in the time it takes for phishing domains to be deregistered after detection. Across all phishing domains, the average time between detection and deregistration is 11.5 days on average, reflecting a relatively short-lived post-detection activity. However, specific domain categories reveal notable discrepancies. Squatted domains persist significantly longer, with an average lifespan of 23 days post-detection. Random-looking domains and impersonating specific branded domains exhibit average post-detection duration of 14.8 days and 19.9 days, respectively.

This prolonged availability of squatted and brand-targeted domains underscores their continued risk in phishing campaigns, as these domains remain accessible to victims even after being blocklisted. The observed differences in deregistration times between maliciously registered domain categories, such as brand-targeted (19.9 days), random-looking (14.8 days), and squatted domains (23 days), may reflect variations in the policies or practices of registrars and hosting providers. These differences could also indicate that attackers exploit specific domain types for their perceived resilience or due to differences in enforcement or takedown mechanisms. These findings reveal critical gaps in enforcement mechanisms, particularly for squatted domains, which outlast other categories by a wide margin.

Takeaway: Maliciously registered domains, especially squatted domains, are key in phishing domains but are deregistered more slowly, averaging 23 days compared to 11.5 days for all phishing domains.

7.3 Comparison Between Blocklists

As shown in Figure 6, detection times vary significantly between APWG and other blocklists, illustrating how quickly each blocklist identifies phishing domains after they have already been detected by APWG. APWG plays a critical role in identifying phishing domains, with domains on its blocklist having an average detection time of 277.3 days and a median detection time of 42.4 days.

In contrast, other blocklists show considerable delays in detecting these same domains. For instance, Phishunt.io has an average detection delay of 676.1 days and a median of 930.8 days after APWG's detection, indicating significant lag. Conversely, blocklists like PhishTank and OpenPhish demonstrate faster detection times, with PhishTank averaging 167.7 days and a median of 4.4 days, while OpenPhish averages 257.9 days and a median of 4.1 days after

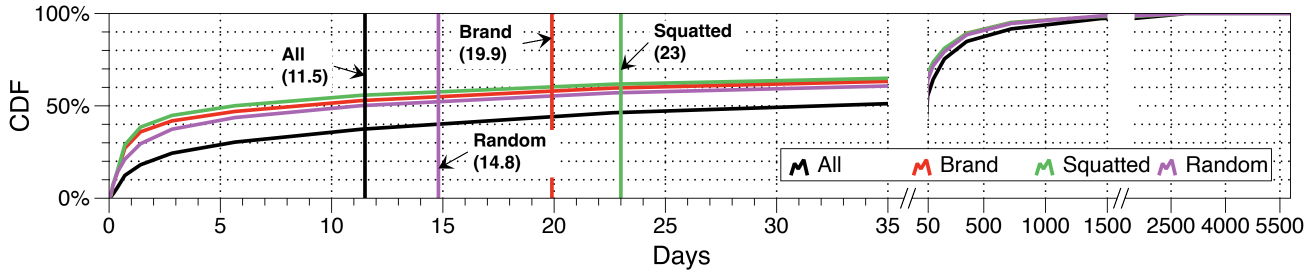


Figure 7: Days Between Detection and Last Seen. Vertical bars show the last seen timestamp from the zone file by each type of maliciously registered domain.

APWG detection. `Malware-filter` and `PhishStats` also detect domains relatively quickly, with median delays of 3.7 and 2.3 days, respectively, despite higher average delays of 255.6 and 141.9 days.

`Phishing.Database` shows mixed results, with an average detection delay of 388.5 days but a stronger median delay of 64.4 days. These findings demonstrate that APWG consistently detects phishing domains earlier than all other blocklists in our dataset. However, the variability in detection delays across blocklists highlights the need for improved synchronization and data sharing to reduce detection gaps and enhance phishing defense coverage. APWG's early detection could be further leveraged to accelerate response times across the ecosystem.

> **Takeaway:** APWG consistently detects phishing domains earlier than other blocklists, but significant variability in detection delays across blocklists underscores the need for improved synchronization and data sharing to enhance timely phishing defense and reduce attacker impact.

8 Discussion

Based on our analysis, we outline limitations and provide recommendations to guide future research efforts.

Limitation. During our verification step, a small number of domains may fall outside our defined malicious domain classification categories. While we conducted manual verification to ensure the accuracy of our results, it is still possible that a few domains can exhibit characteristics that do not align with our predefined criteria.

Recommendation. There have been various approaches to understanding how phishing attackers exploit domain registration systems and policies to register malicious domains. Previous research has proposed multiple strategies to address this issue, but the persistence of maliciously registered domains indicates that existing efforts remain insufficient. Several approaches have been discussed in prior work to prevent attackers from registering malicious domains:

- **Stricter Verification Processes**: Implementing enhanced registrant verification during domain registration, such as requiring government-issued identification or multi-factor authentication, to ensure the legitimacy of registrants.
- **Monitoring and Reporting Systems**: Developing real-time monitoring tools to detect suspicious registration patterns, such as bulk registrations or domains containing high-risk keywords, and establishing automated reporting mechanisms to notify registrars and relevant authorities.
- **Registrar Accountability**: Encouraging or mandating registrars to adopt anti-abuse policies, *e.g.*, proactive detection measures and swift suspension of flagged domains.
- **Global Collaboration**: Promoting coordinated efforts between registries, registrars, security organizations, and governments to standardize policies and share intelligence on malicious registration practices.
- **Policy Enforcement for Low-Cost TLDs**: Strengthening oversight for TLDs with low registration costs, which are often exploited by attackers.

However, due to the decentralized nature of domain registration systems and varying policies among registries and registrars, it is challenging to implement a generalized defense mechanism. Our analysis aims to reiterate these recommendations and emphasize the urgent need for domain registries and registrars to defend against malicious domains proactively. By adopting these measures, stakeholders can significantly reduce phishing attackers' exploitation of domain registration systems.

Ethics. Our methods emphasize ethical responsibility while upholding scientific rigor in analyzing real-world phishing domains. The data collection process including crawling DNS data and registration data (*e.g.*, RDAP), strictly adheres to established ethical guidelines, utilizing phishing URLs sourced from blocklist feeds explicitly made available for research purposes.

9 Related Work

The number of reports showed the trend of phishing domains and examined phishing websites. However, the characteristics of DNS settings of phishing domains are not well studied.

Coverage of TLDs in Phishing Domains. Previous work [46] has a narrow focus on three specific ccTLDs, while our work broadens the analysis to include all TLDs (gTLDs and ccTLDs), offering a more comprehensive understanding of phishing trends across a diverse range of domain spaces. While the prior study [46] focused on identifying impersonated domains, our work delves into how long these phishing domains remain active post-registration, comparing this lifespan to detection delays on blocklists (*e.g.*, APWG). Furthermore, our work enhances the analysis by examining the characteristics of specific targeted brands in phishing domains. Our work also goes beyond registration trends by exploring the influence of economic factors, such as whether cheaper TLDs contribute to the trend of phishing domains.

Lifecycle and Classification of Phishing Domains. The previous study [44] introduced a classification method that distinguishes between compromised and maliciously registered domains using 32 extracted features. However, their analysis is restricted to identifying malicious domains, leaving a gap in understanding domain behaviors beyond real-world phishing datasets. Our work builds upon COMAR [44] by applying its method more broadly to understand maliciously registered domains with real-world phishing datasets. Similarly, while prior work [28] examined bulk registrations, it was limited to five months of `.com` TLD data. Our work builds upon these studies by analyzing *multiple* gTLDs and ccTLDs, providing comprehensive insights into how maliciously registered domains behave differently from compromised domains across various TLDs and targeted brands.

Registration Patterns and Longevity of Phishing Domains. Previous research [51] reveals that 75% of victims access phishing webpages before they are detected. Building on this, our work examines the lifespan of phishing domains, compares the lifespans across different targeted brands, and analyzes various types of maliciously registered domains to uncover patterns and strategies used by attackers.

DNS Behavior and Phishing Detection Delays. Previous work [26] found that 55% of malicious domains are first detected in spam campaigns over a day after registration. Building on this, our study provides a more comprehensive analysis of phishing domains' lifecycles, spanning from registration to detection and deregistration. By examining the delay between domain registration and blocklist detection, we offer a clearer understanding of detection timelines for both maliciously registered and compromised domains, highlighting gaps in current detection mechanisms.

10 Conclusion

This study provides a comprehensive analysis of phishing domains, focusing on maliciously registered domains, DNS behaviors, and detection timelines. We find that 66.1% of domains are maliciously registered, with attackers favoring low-cost TLDs like `.top` and `.tk`, and frequently using hosting services like AWS. Maliciously registered domains are detected faster than compromised ones (median 16.3 vs. 86 days), yet significant delays persist across blocklists. Some domains could take over a year to be listed. Our findings highlight the need for improved blocklist synchronization and monitoring of widely abused TLDs to mitigate phishing threats effectively.

References

[1] FBI's IC3 Report. https://www.proofpoint.com/us/blog/email-and-cloud-threats/fbis-ic3-report-losses-cybercrime-surpass-125-billion-new-record, March 2024. (Accessed on 11/20/2024).
[2] Aceville. Dnspod. https://www.dnspod.com/, 11 2024. (Accessed on 11/19/2024).
[3] Antonia Affinito, Raffaele Sommese, Gautam Akiwate, Stefan Savage, kc claffy, Geoffrey M Voelker, Alessio Botta, and Mattijs Jonker. Domain name lifetimes: Baseline and threats. In *TMA*, 2022.
[4] Alibaba. Domain name bulk registration-basic edition. https://check.aliyun.com/domain/bulk-search/basic.htm, 11 2024. (Accessed on 11/16/2024).
[5] Alibaba. New user discount! only $0.5 - alibaba cloud. https://www.alibabacloud.com/ko/domain/1dollar?_p_lc=1&spm=a3c0i.145322.1761468070.2.522a4635pLdxUS, 11 2024. (Accessed on 11/16/2024).
[6] APWG. Apwg | the apwg ecrime exchange (ecx). https://apwg.org/ecx/, 11 2024. (Accessed on 11/17/2024).
[7] Archive. Wayback machine. https://web.archive.org/, 11 2024. (Accessed on 11/20/2024).
[8] Greg Belding. Phishing: Reputational damages | infosec. https://www.infosecinstitute.com/resources/phishing/reputational-damages/, 2020. (Accessed on 11/20/2024).
[9] Leyla Bilge, Engin Kirda, Christopher Kruegel, and Marco Balduzzi. EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis. In *Proc. of the Network and Distributed System Security (NDSS)*, 2011.
[10] CAIDA. home - dzdb. https://dzdb.caida.org/, 11 2024. (Accessed on 11/15/2024).
[11] Davide Canali, Davide Balzarotti, and Aurélien Francillon. The role of web hosting providers in detecting compromised websites. In *Proceedings of the 22nd international conference on World Wide Web*, pages 177–188, 2013.
[12] Alibaba Cloud. Alibaba cloud. https://www.alibabacloud.com/, 11 2024. (Accessed on 11/19/2024).
[13] Cloudflare. Cloudflare free ssl/tls. https://www.cloudflare.com/application-services/products/ssl/, 11 2024. (Accessed on 11/20/2024).
[14] curbengh. curbengh/malware-filter: Mirror of https://gitlab.com/malware-filter/malware-filter. https://github.com/curbengh/malware-filter, 11 2024. (Accessed on 11/05/2024).
[15] David Dagon, Niels Provos, Christopher P Lee, and Wenke Lee. Corrupted DNS Resolution Paths: The Rise of a Malicious Resolution Authority. In *Proc. of the Annual Network and Distributed System Security Symposium (NDSS)*, 2008.
[16] Ravindu De Silva, Mohamed Nabeel, Charith Elvitigala, Issa Khalil, Ting Yu, and Chamath Keppitiyagama. Compromised or {Attacker-Owned}: A large scale classification and study of hosting domains of malicious {URLs}. In *30th USENIX security symposium (USENIX security 21)*, pages 3721–3738, 2021.
[17] DomainTools. Introducing dnsdb 2.0 | passive dns | domaintools. https://www.domaintools.com/products/farsight-dnsdb/, 11 2024. (Accessed on 11/15/2024).
[18] Dynabot. Buy a domain name - register, manage, and save more | dynadot. https://www.dynadot.com/, 11 2024. (Accessed on 11/19/2024).
[19] elceef. elceef/dnstwist: Domain name permutation engine for detecting homograph phishing attacks, typo squatting, and brand impersonation. https://github.com/elceef/dnstwist, 09 2024. (Accessed on 11/16/2024).
[20] Fox-IT. Using anomaly detection to find malicious domains – fox-it international blog. https://blog.fox-it.com/2019/06/11/using-anomaly-detection-to-find-malicious-domains/, 06 2019. (Accessed on 11/16/2024).
[21] Tillson Galloway, Kleanthis Karakolios, Zane Ma, Roberto Perdisci, Angelos Keromytis, and Manos Antonakakis. Practical Attacks Against DNS Reputation Systems. In *Proc. of the IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, 2024.
[22] Gname. Gname | buy domain names, websites, hosting, cloud products. https://www.gname.com/, 11 2024. (Accessed on 11/19/2024).
[23] GoDaddy. Godaddy. https://www.godaddy.com, 11 2024. (Accessed on 11/19/2024).
[24] Google. Safe browsing – google safe browsing. https://safebrowsing.google.com/, 11 2024. (Accessed on 11/19/2024).
[25] Anders Gorboe. Detection of fake domain names in e-mails. Master's thesis, OsloMet-storbyuniversitetet, 2022.
[26] Shuang Hao, Nick Feamster, and Ramakant Pandrangi. Monitoring the initial dns behavior of malicious domains. In *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*, pages 269–278, 2011.
[27] Shuang Hao, Alex Kantchelian, Brad Miller, Vern Paxson, and Nick Feamster. Predator: proactive recognition and elimination of domain abuse at time-of-registration. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pages 1568–1579, 2016.
[28] Shuang Hao, Matthew Thomas, Vern Paxson, Nick Feamster, Christian Kreibich, Chris Grier, and Scott Hollenbeck. Understanding the domain registration behavior of spammers. In *Proceedings of the 2013 conference on Internet measurement conference*, pages 63–76, 2013.
[29] ICANN. About zone file access - icann. https://www.icann.org/resources/pages/zfa-2013-06-28-en, 06 2013. (Accessed on 11/15/2024).
[30] ICANN. At-large - topic: New gtlds. https://atlarge.icann.org/topics/new-gtlds, 11 2024. (Accessed on 11/17/2024).
[31] ICANN. Help | centralized zone data service. https://czds.icann.org/help, 11 2024. (Accessed on 11/15/2024).
[32] Interisle. Phishing landscape 2024: An annual study of the scope and distribution of phishing — interisle consulting group. https://interisle.net/insights/phishing-landscape-2024-an-annual-study-of-the-scope-and-distribution-of-phishing, 07 2024. (Accessed on 11/17/2024).
[33] ionos. Dns ttl best practices: Understanding and configuring dns ttl - ionos. https://www.ionos.com/digitalguide/server/configuration/understanding-and-configuring-dns-ttl/, 11 2024. (Accessed on 11/19/2024).
[34] IPinfo. Ip summarization & data visualization - ipinfo.io. https://ipinfo.io/tools/summarize-ips, 11 2024. (Accessed on 11/22/2024).
[35] Keshav Kaushik, Sahajpreet Singh, Saksham Garg, Sarthak Singhal, and Shambhavi Pandey. Exploring the mechanisms of phishing. *Computer Fraud & Security*, 2021(11):14–19, 2021.
[36] Doowon Kim, Haehyun Cho, Yonghwi Kwon, Adam Doupé, Sooel Son, Gail-Joon Ahn, and Tudor Dumitras. Security analysis on practices of certificate authorities in the https phishing ecosystem. In *Proc. of the ACM Asia Conference on Computer and Communications Security*, 2021.

[37] Maciej Korczynski, Maarten Wullink, Samaneh Tajalizadehkhoob, Giovane CM Moura, Arman Noroozian, Drew Bagley, and Cristian Hesselman. Cybercrime after the sunrise: A statistical analysis of dns abuse in new gtlds. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, pages 609–623, 2018.
[38] Kreb. Sued by meta, freenom halts domain registrations – krebs on security. https://krebsonsecurity.com/2023/03/sued-by-meta-freenom-halts-domain-registrations/, 03 2023. (Accessed on 11/20/2024).
[39] Kyungchan Lim, Jaehwan Park, and Doowon Kim. Phishing Vs. Legit: Comparative Analysis of Client-Side Resources of Phishing and Target Brand Websites. In *Proc. of the international World Wide Web conference (WWW)*, 2024.
[40] Yun Lin, Ruofan Liu, Dinil Mon Divakaran, Jun Yang Ng, Qing Zhou Chan, Yiwen Lu, Yuxuan Si, Fan Zhang, and Jin Song Dong. Phishpedia: A hybrid deep learning based approach to visually identify phishing webpages. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 3793–3810, 2021.
[41] Ruofan Liu, Yun Lin, Xiwen Teoh, Gongshen Liu, Zhiyong Huang, and Jin Song Dong. Less defined knowledge and more true alarms: Reference-based phishing detection without a pre-defined reference list. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 523–540, 2024.
[42] Ruofan Liu, Yun Lin, Xianglin Yang, Siang Hwee Ng, Dinil Mon Divakaran, and Jin Song Dong. Inferring phishing intention via webpage appearance and dynamics: A deep vision based approach. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 1633–1650, 2022.
[43] Ruofan Liu, Yun Lin, Yifan Zhang, Penn Han Lee, and Jin Song Dong. Knowledge expansion and counterfactual interaction for {Reference-Based} phishing detection. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 4139–4156, 2023.
[44] Sourena Maroofi, Maciej Korczyński, Cristian Hesselman, Benoit Ampeau, and Andrzej Duda. Comar: classification of compromised versus maliciously registered domains. In *2020 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 607–623. IEEE, 2020.
[45] mitchellkrogza. mitchellkrogza/phishing.database: Phishing domains, urls websites and threats database. we use the pyfunceble testing tool to validate the status of all known phishing domains and provide stats to reveal how many unique domains used for phishing are still active. https://github.com/mitchellkrogza/Phishing.Database, 11 2024. (Accessed on 11/05/2024).
[46] Giovane CM Moura, Thomas Daniels, Maarten Bosteels, Sebastian Castro, Moritz Müller, Thymen Wabeke, Thijs van den Hout, Maciej Korczyński, and Georgios Smaragdakis. Characterizing and mitigating phishing attacks at ccTLD scale (extended). 2024.
[47] Namesilo. Low-cost domain names & hosting from $0.99 | namesilo. https://www.namesilo.com/, 11 2024. (Accessed on 11/19/2024).
[48] Adam Oest, Yeganeh Safaei, Adam Doupé, Gail-Joon Ahn, Brad Wardman, and Kevin Tyers. Phishfarm: A scalable framework for measuring the effectiveness of evasion techniques against browser phishing blacklists. In *Proc. of the IEEE Symposium on Security and Privacy*, 2019.
[49] Adam Oest, Yeganeh Safaei, Penghui Zhang, Brad Wardman, Kevin Tyers, Yan Shoshitaishvili, and Adam Doupé. {PhishTime}: Continuous longitudinal measurement of the effectiveness of anti-phishing blacklists. In *Proc. of the USENIX Security Symposium*, 2020.
[50] Adam Oest, Yeganeh Safei, Adam Doupé, Gail-Joon Ahn, Brad Wardman, and Gary Warner. Inside a phisher's mind: Understanding the anti-phishing ecosystem through phishing kit analysis. In *Proc. of the APWG Symposium on Electronic Crime Research*, 2018.
[51] Adam Oest, Penghui Zhang, Brad Wardman, Eric Nunes, Jakub Burgis, Ali Zand, Kurt Thomas, Adam Doupé, and Gail-Joon Ahn. Sunrise to sunset: Analyzing the end-to-end life cycle and effectiveness of phishing attacks at scale. In *29th {USENIX} Security Symposium ({USENIX} Security 20)*, 2020.
[52] openphish. Openphish - phishing intelligence. https://openphish.com/, 11 2024. (Accessed on 11/05/2024).
[53] OZON. OZON Marketplace. https://www.ozon.ru/, 11 2024. (Accessed on 11/19/2024).
[54] phishstats. Phishstats. https://phishstats.info/, 11 2024. (Accessed on 11/05/2024).
[55] phishtank. Phishtank | join the fight against phishing. https://phishtank.org/, 11 2024. (Accessed on 11/05/2024).
[56] phishunt. phishunt - free phishings and scams feed. https://phishunt.io/, 11 2024. (Accessed on 11/05/2024).
[57] RDAP. Rdap.org. https://about.rdap.org/, 11 2024. (Accessed on 11/15/2024).
[58] Joe St Sauver. Automating detection of "random-looking" algorithmic domain names - domaintools | start here. know now. https://www.domaintools.com/resources/blog/automating-detection-of-random-looking-algorithmic-domain-names/, 05 2019. (Accessed on 11/12/2024).
[59] Sav. Sav. https://www.sav.com/, 11 2024. (Accessed on 11/19/2024).
[60] SCOWL. Scowl custom list/dictionary creator. http://app.aspell.net/create, 11 2024. (Accessed on 11/20/2024).
[61] Ruchi Sharma, Bhag Dei Thakur, Neelam Kaushik, and Purnima Chauhan. Securing the web: A study on look-alike domain detection using open-source intelligence tools. *Journal of Information Security and Cybercrimes Research*, 7(1):05–28, 2024.
[62] Network Solutions. Domain name | network solutions. https://www.networksolutions.com, 11 2024. (Accessed on 11/19/2024).
[63] tldlist. Compare prices of all top-level domains | tld-list. https://tld-list.com/, 11 2024. (Accessed on 11/15/2024).
[64] Tranco. A research-oriented top sites ranking hardened against manipulation - tranco. https://tranco-list.eu/, 11 2024. (Accessed on 11/20/2024).
[65] USPS. Welcome | usps. https://www.usps.com/, 11 2024. (Accessed on 11/19/2024).
[66] Vorsk. home - dns coffee. https://dns.coffee/, 11 2024. (Accessed on 11/15/2024).

A Example of Bulk Registration.

As shown in Figure 8, AlibabaCloud provides extensive features that facilitate bulk domain registration while offering promotional pricing for new users. The platform advertises and combines several capabilities that make bulk registration highly accessible: deeply discounted pricing for new users (domains for as low as $0.5), explicit bulk management tools allowing simultaneous registration of multiple domains, and automation tools for managing multiple domains. While these features serve legitimate business purposes, they can be exploited by attackers to register multiple phishing domains efficiently at minimal cost. The combination of bulk registration capabilities, automation tools, and aggressive pricing promotions makes the platform particularly attractive for malicious actors orchestrating large-scale phishing campaigns.

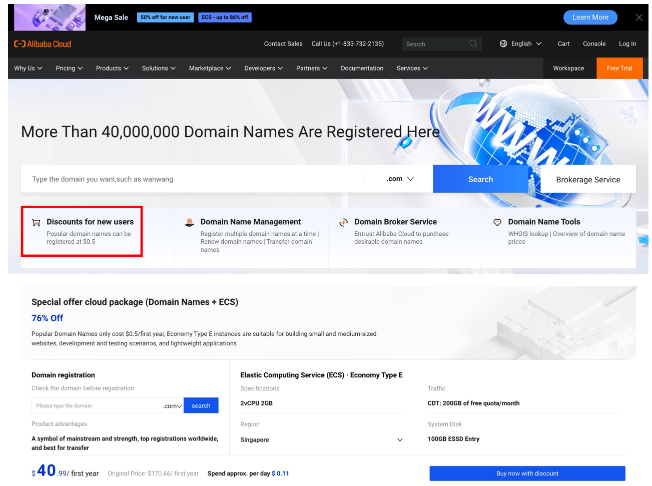


Figure 8: Alibaba Cloud offers promotion and allows bulk registration.