Game of Registrars: An Empirical Analysis of Post-Expiration Domain Name Takeovers

Tobias Lauinger, ***Northeastern University;*** **Abdelberi Chaabane,** ***Nokia Bell Labs;***
Ahmet Salih Buyukkayhan, ***Northeastern University;*** **Kaan Onarlioglu,** ***www.onarlioglu.com;***
William Robertson, ***Northeastern University***

https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/lauinger

This paper is included in the Proceedings of the
26th USENIX Security Symposium

August 16–18, 2017 • Vancouver, BC, Canada

ISBN 978-1-931971-40-9

Open access to the Proceedings of the
26th USENIX Security Symposium
is sponsored by USENIX

Game of Registrars: An Empirical Analysis of Post-Expiration Domain Name Takeovers

Tobias Lauinger
Northeastern University

Abdelberi Chaabane
Nokia Bell Labs

Ahmet Salih Buyukkayhan
Northeastern University

Kaan Onarlioglu
www.onarlioglu.com

William Robertson
Northeastern University

Abstract

Every day, hundreds of thousands of Internet domain names are abandoned by their owners and become available for re-registration. Yet, there appears to be enough residual value and demand from domain speculators to give rise to a highly competitive ecosystem of *drop-catch* services that race to be the first to re-register potentially desirable domain names in the very instant the old registration is deleted. To pre-empt the competitive (and uncertain) race to re-registration, some registrars sell their own customers' expired domains *pre-release*, that is, even before the names are returned to general availability.

These practices are not without controversy, and can have serious security consequences. In this paper, we present an empirical analysis of these two kinds of post-expiration domain ownership changes.We find that 10 % of all `com` domains are re-registered on the same day as their old registration is deleted. In the case of `org`, over 50 % of re-registrations on the deletion day occur during only 30 s. Furthermore, drop-catch services control over 75 % of accredited domain registrars and cause more than 80 % of domain creation attempts, but represent at most 9.5 % of successful domain creations. These findings highlight a significant demand for expired domains, and hint at highly competitive re-registrations.

Our work sheds light on various questionable practices in an opaque ecosystem. The implications go beyond the annoyance of websites turned into "Internet graffiti" [26], as domain ownership changes have the potential to circumvent established security mechanisms.

1 Introduction

Domain names are a key part of linking to content on the Web, and they have an equally central role in naming services on the Internet, such as in email addresses. A large number of security mechanisms and protocols have been devised that rely on domains to designate distinct zones of authority or trust. For example, controlling a domain name is often equivalent to gaining access to additional resources [44]. An assumption common to all these approaches is that domain ownership is constant and perpetual. However, in actuality this is not true as domain name registrations must be renewed and paid for on a yearly basis. In fact, hundreds of thousands of expired domain names are deleted each day (e.g., over 75 k per day in the popular `com` zone alone [24]).

Once a domain name has been deleted, it can be re-registered by any interested party on a first-come, first-served basis. Schlamp et al. [44] showed how such re-registrations can be used to take over protected resources associated with these domains. Nikiforakis et al. [42] discussed websites still attempting to include JavaScript code from third-party domains long after they had expired, allowing attackers to inject code into these sites. Lever et al. [33] measured more formally how often re-registered domains were associated with malicious behaviour. However, by focussing on certain kinds of risk or malice, these studies do not illustrate the full scope of the issue.

We argue that the problem goes beyond specific cases of abuse related to re-registered domains. It also includes the much broader and more frequent category of *undesirable behaviour* akin to topics thoroughly studied by the security community, such as spam [32], search engine poisoning [49], ISPs hijacking NXDOMAIN DNS responses [50], domain parking [2, 48], typo-squatting [1, 37, 47], and reuse of social media profile names [35, 36]. Re-registered domains appear to be predominantly used for speculation and monetisation purposes, taking advantage of the residual traffic still reaching the domains. Users who follow links from third-party websites or type in an address that they remember are taken to a new incarnation of the site that can be arbitrarily different from the service that they actually wish to visit. In Section 4.4, we show that a majority of re-registered domains are parked and host nothing but advertisements. ICANN called this undesirable practice "a form of Inter-

net graffiti" [26]; domain parking is also known to pose higher-than-average risks to visitors [48].

We believe it is important for the security community to better understand the big picture of domain ownership transfers and the implications for users, Internet abuse, and defences thereof. This paper provides a quantitative analysis of the "recycling" of expired domain names. We show that this is a frequent phenomenon, causing a range of negative side effects as companies compete with each other while catering to the demand for expired domains.

There are four distinct scenarios in which domains can change owners: When the current owner sells to a new owner while the domain registration is active; when the domain's sponsoring registrar sells the domain to a new owner while the domain registration is expired but before control of the domain is returned to the registry (*pre-release*); as an instant re-registration in the very moment the old registration is deleted, using a *drop-catch* service; or as a conventional domain registration at any later time using any domain name registrar. Regular domain sales are authorised by the owner of the domain and therefore less of a concern from an abuse perspective. Medium to long-term domain re-registrations have been studied before [29, 22]. Pre-release and drop-catch domain ownership transfers, however, are barely mentioned in the literature, and we are not aware of any systematic measurement or quantification of these phenomena.

There is an entire ecosystem of services attempting to monetise and profit from expired domains. Many domain registrars such as GoDaddy auction off their own customers' expired domains (without their collaboration); when sold, these domains maintain their current registration and are simply made over to the new owner. From a security perspective, such pre-release domains are problematic because they retain their original creation dates and exhibit only very limited cues as to the new ownership. For instance, pre-release domains subvert proactive creation-time domain blacklisting mechanisms such as Predator [21], which is related to a similar technique used by the commercial Spamhaus blacklist, because the ownership change does not involve a new registration. This example illustrates the need for a thorough study of how commonly pre-release domains are available and sold.

Once expired domains are deleted, they can be re-registered on a first-come, first-served basis, and these re-registrations can be quite competitive. So-called *drop-catch* services race to be the first to re-register expired domain names in the very moment they become available. During a daily phenomenon that is called "the drop," they flood the registry's systems with registration requests, something previously described as "the world's largest legal denial of service attack" [8]. In order to gain an advantage over their competition, drop-catch services reverse-engineer details of the drop [8, 28] and place their own systems in an "optimal strategical location" [4] physically close to the registry; these optimisations resemble high-frequency trading in the financial industry. Drop-catch services are not without controversy. Some registries actively discourage the practice (e.g., registrars are penalised for failed `uk` registration requests [8]), while others at least implicitly encourage or facilitate it (e.g., Verisign makes available to its registrars lists of `com` and `net` domains that are about to be deleted).

The extent and process of the drop are publicly known only in abstract terms as each drop-catch service aims to maintain their competitive position. In this paper, we conduct the first measurement study of the drop and provide as much detail as is possible from an outside vantage point. Furthermore, we characterise the extent and competitiveness of drop-catch re-registrations on "day 0," that is, the day an expired domain name is deleted.

We find that a surprisingly large fraction of deleted domains (10 % of `com`) is re-registered *on the same day*. In the case of `org`, the drop lasts only about 30 seconds, but accounts for more than half of all same-day re-registrations of deleted domains. These results show that re-registrations are frequent and highly competitive. Despite the significantly higher price, there is a large demand for drop-catch domains. In fact, there seems to be an arms race between drop-catch services that has been intensifying recently, with the Top 3 now controlling 75 % of accredited registrars. Drop-catch causes at least 80 % of domain creation attempts, yet only a tiny fraction are eventually successful. The higher prices paid for drop-catch domains suggest that their new owners consider them to be valuable; however, in our cursory analysis of domain uses, we show that most re-registered drop-catch domains contain nothing but advertisements and parking pages, suggesting monetisation through residual traffic and speculative re-registrations. Our findings raise the question of whether these uses justify the risks associated with domain ownership changes without the explicit consent of the prior registrant; they furthermore illustrate that security mechanisms must account for domain deletions and re-registrations as a frequent phenomenon (e.g., more than 20 % of all `com` domains are deleted each year, and out of those, 10 % are re-registered immediately by a new owner, and many more at a later time).

Our work makes the following contributions:

- We call attention to widespread "recycling" of used domains despite relatively high prices and measure the extent of the issue *as a whole*, instead of simply focussing on specific types of detected abuse.
- We describe little-known ways domain ownership can change, and are the first to quantify the secretive ecosystem of drop-catch services and their daily race to take over deleted domains. We use a variety of

public data sources to confirm the existence of a phenomenon so far described only anecdotally.

- We show that same-day domain takeovers are frequent and competitive, using a full sample of all domains deleted from four popular zones during a four-week period in 2016 (over 4 million domains).
- We quantify the inordinate impact that drop-catch services have on the domain registration ecosystem, accounting for over 75 % of accredited registrars and over 80 % of domain creation attempts, but at most 9.5 % of successful domain creations.
- We discuss how certain registrars exploit grace periods to minimise their financial risk when attempting to sell pre-release domains or proactively re-registered drop-catch domains, similar to the now banned practice of domain tasting [6, 27].

2 Background & Related Work

Names in the Domain Name System (DNS) are structured hierarchically. Top-level domains (TLDs) such as `com` or `net` are created by the Internet Corporation for Assigned Names and Numbers (ICANN) and then delegated for day-to-day operation to a *registry* such as Verisign. Each registry maintains a directory of the registered second-level names and their authoritative name servers, called a DNS *zone*. Registries delegate billing and customer support to ICANN-accredited *registrars*, companies such as GoDaddy or Gandi, which sell domain names to their customers. The Internet Assigned Numbers Authority (IANA) maintains a list of all accredited registrars and their globally unique IDs [23]. Details about the activity of these registrars in each zone are available in the monthly reports that registries must file with ICANN, and that are made public after a three-month delay [24].

2.1 Domain Lifecycle

Domains are registered for a period of one or more years. If a domain is not renewed before its expiration date, it goes through a series of phases that permit late renewals before the domain is ultimately deleted. Figure 1 shows a simplified domain state diagramme taken from [29]. For the purposes of this paper, it is sufficient to know that domains not explicitly renewed or deleted before their expiration date are automatically renewed by the registry, giving the registrar a 45-day *auto-renew grace period* to undo this automatic renewal before becoming liable for the renewal fees. The details of how this grace period affects the domain and its original owner depend on each registrar's policies. Typically, registrars either deactivate the domain or point it to a parking site to alert the owner that the domain can still be renewed. Unless otherwise requested by the owner of the expired domain, registrars typically delete it shortly before the end of the 45-day *auto-renew grace period* in order not to incur the registry's renewal fee. Such domains enter a 30-day *redemption period* during which the domain is deactivated and "locked" by the registry in the sense that the only allowed modification is renewal by the original owner, for an increased fee. Domains not recovered during the *redemption period* transition into the *pending delete* state, which means that these registrations will be deleted after 5 days and the domains can be re-registered by any interested party on a first-come, first-served basis.

Figure 2 summarises a domain's most typical expiration phases on a timeline. Expired domains can change owners during two points in time: *Pre-release domains* can be sold and transferred to a new owner during the *auto-renew grace period*; *pending delete domains* can be re-registered by a drop-catch service directly after deletion, or manually at any later point, all provided that the domain has not already changed owners beforehand.

2.2 Pre-Release Domain Sales

During the *auto-renew* grace period, even though the expiration date has already passed, registrars maintain control over the domain. ICANN and the registries appear to give registrars some flexibility in how they manage this period, with the result that different registrars implement a range of varying policies that may or may not be favourable to the registrant of the expiring domain. Some registrars such as Gandi give their customers the full 45 days for late renewals without additional fees [15], whereas other registrars begin charging increased late renewal fees or attempt to sell the domain to a new owner. GoDaddy, for example, begins charging customers an increased late renewal fee on the 19$^{\text{th}}$ day after expiration, and puts the domain name up for auction beginning on the 26$^{\text{th}}$ day [17]. While GoDaddy operates their own domain name auction service, other registrars such as Moniker or Tucows partner with third-party platforms such as SnapNames [46]. These auctions allow any interested party to bid for expiring names and potentially acquire them, subject to the original registrant not exercising their right to renew the domain. If a domain is sold, the new owner pays for the renewal as well as auction fees and the sponsoring registrar changes the domain's ownership information to the new owner. The domain remains under the management of the registrar and keeps its original metadata such as the registration creation date. From a domain management point of view, this process is the same as what would happen if the previous owner had sold the domain to a new owner, except that the previous owner does not in fact participate in or benefit from the pre-release sale, since all proceeds go to the registrar and

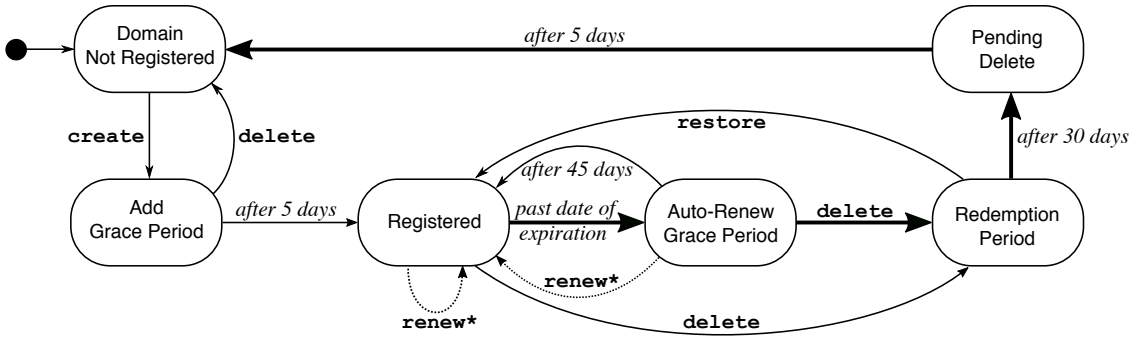

Figure 1: Diagramme from [29] showing domain states and transitions due to `commands` issued by the registrar, or *automatic* transitions if no command is issued before the deadline. If a domain is not `deleted` or `renew`ed by the registrar before the expiration date, the registry automatically renews it for a year. *Additional states for `renew` and domain transfers omitted.

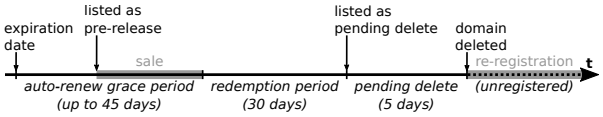

Figure 2: Timeline of domain expiration with a *pre-release* sale opportunity during the *auto-renew grace period* and a re-registration opportunity after the domain has been deleted (*drop-catch* re-registrations occur instantly after deletion).

auction platform. The entire auction process takes place during the duration of the *auto-renew grace period* when registrars hold the domains for free. Unsold domains can be deleted before they incur any cost at the registry, which means that registrars run a negligible financial risk when they attempt to sell their customers' expired domains.

2.3 Drop-Catch Domain Re-Registrations

While the general process of domain expiration depicted in Figure 1 is very similar for the generic TLDs, the exact procedure of domain deletion at the end of the *pending delete* period may differ from registry to registry. In the following description, we focus on the `com` and `net` zones operated by Verisign because they are the most popular and have most details available in various online sources [8, 28, 13]. According to these sources, each day Verisign makes available to its registrars a list of all domains that just entered the *pending delete* period and will become available for re-registration five days later, along with popularity data derived from traffic to the zone's authoritative DNS servers. Deletion of domains follows a somewhat predictable procedure that is also called "the drop." Beginning each day at 2pm ET, Verisign's systems iterate over the "dropping" domain names in a certain order and change their status from *registered* to *available* one by one, with the whole process lasting up to an hour.

Since deleted domains can be re-registered on a first-come, first-served basis, to maximise the probability of "catching" a sought-after domain, it is essential to predict when exactly it will "drop" and place the re-registration request in a timely manner. For popular domains, it is not very promising to attempt to do so manually, since a number of *drop-catch* services specialise in automatic re-registration of deleted domains in the very moment they become available. These services accept backorders from customers who are interested in an already registered domain and attempt to re-register the domain if it is ever deleted. Around the deletion window, drop-catch services flood the registry with registration requests, most of which can be expected to fail because the domain has either not been deleted yet, or it has already been re-registered by a competitor. Drop-catch services attempt to reverse engineer the registry's deletion process in order to use their resources more efficiently and gain an advantage over their competition. Furthermore, drop-catch services are said to use multiple (rate-limited) registrar access credentials and place their servers physically close to the registry's systems [4, 8, 28], similar to common practices in high frequency trading in the financial industry.

In contrast to pre-release domain sales, drop-catch services do not control the domain when an order is placed and cannot guarantee that they will be able to obtain it. The starting price of a drop-catch domain can be up to ten times the regular annual registration fee. If a drop-catch service successfully obtains a domain and multiple customers had placed an order, the winner is typically determined in a three-day private auction. Since such domains were deleted (even if only for fractions of a second), their metadata looks like that of a newly registered domain, without any trace of the prior registration instance.

2.4 Domain Tasting

Figure 1 shows that newly registered domains start in a five-day *add grace period* during which the domain registration can be cancelled at no cost. While intended to address accidental domain registrations such as typing errors, this grace period led to wide-spread abuse, so-called

domain tasting, which consists in domain speculators tentatively registering a domain with the sole purpose of testing how much traffic it would receive, and deleting the domain if the observed traffic did not warrant the registration fee. In related work, Coull et al. [6] showed that domain tasting accounted for 76 % of all daily domain creations. After 2008/2009, when ICANN implemented policies penalising registrars for excessive tasting, the frequency of the phenomenon declined by 99.7 % [27]. We will show in Section 4.6 that in a fashion similar to pre-release sales, at least one drop-catch service makes use of domain tasting to tentatively register domain names and delete them at no cost when it cannot find a buyer.

2.5 Related Work

Prior research in the area of domain registrations includes the work on registration intent by Halvorson et al. [18, 19, 20]. Schlamp et al. [44] describe an attack to take over protected resources by re-registering the expired domains of email addresses. Nikiforakis et al. [42] study inclusions of third-party JavaScript code in websites and find dependencies loaded from expired domain names, which could be re-registered for code injection attacks. Attackers have also been reported to re-register expired domains that built up a good reputation [5, 22, 33].

Although unrelated to domains, Mariconti et al. [35, 36] show that similar risks of trust abuse exist on social networks that allow abandoned profile names to be reused.

Two works present a more systematic examination of domain re-registrations: Hao et al. [22] investigate characteristic registration patterns of spam domains and find that among re-registered domains, those later used for spamming tend to be registered faster than non-malicious domains. They then use several registration-time features to predict which domains are likely to be used for malicious purposes [21]. Lever et al. [33] analyse the maliciousness of domains before and after re-registration with a focus on when malicious behaviour occurs, not when or why a domain is re-registered. In several case studies, they recount concrete security issues that arose from expired (and re-registered) domain names of name servers, email addresses, software repositories, and spam operations. To automatically detect domain ownership changes, the authors propose Alembic, an algorithm based on DNS-related features. It is unclear whether pre-release domain sales exhibit DNS signals strong enough to be detected, since such sales might result in only minor changes to the DNS configuration when domains continue to be maintained by the same registrar or hosting company.

In previous work [29], we studied the expiration process of domain names, long-term re-registration probabilities, and ambiguities in WHOIS data. Our analysis at the time was oblivious to the nature of re-registrations. In this paper, we focus on immediate drop-catch re-registrations, and we also characterise related phenomena such as pre-release sales. We are not aware of any prior work that has studied the pre-release and drop-catch ecosystems.

3 Methodology

To study post-expiration ownership changes of domain names, we need to know which domains are available for pre-release sale or drop-catch re-registration, and track their status to discover the outcome.

3.1 Domain Availability Lists

Most pre-release and drop-catch services publish lists of imminently available domains so that prospective buyers can scout them for interesting inventory. We downloaded these lists daily as the starting point for our analysis.

3.1.1 Pre-Release

We downloaded pre-release lists from four large services that sell expiring domains: Dynadot [14], GoDaddy [16], NameJet [40], and SnapNames [45]. These lists contain the names of available pre-release domains along with the date when each auction will close, and sometimes also metadata such as the current bid, the number of participants in the auction, the age of the domain, or traffic data collected by the registrar from a post-expiration parking page that can be used to valuate the domain. While Dynadot and GoDaddy are primarily registrars and appear to re-sell their own customers' expired domains, other services partner with third-party registrars to offer their expiring domain inventory (e.g., the list of partner registrars of SnapNames includes Moniker and Tucows).

3.1.2 Pending Delete

Lists of domains in the *pending delete* state are available from drop-catch services such as Namepal Backorders [3], Domain Graveyard [9], Domain Monster [10], DropCatch [11], Dynadot [14], NameJet [40], Pool [43], and SnapNames [45]. These lists contain the deletion date of each domain, that is, when the domain can be re-registered, and sometimes also traffic data derived from the zone's DNS lookup traffic.

A practical complication when using these lists is that the time zones of dates are sometimes not explicitly stated, and the listed dates sometimes refer to the last time to place an order, whereas in other cases they refer to the actual deletion date. In contrast to pre-release lists, pending delete lists do not contain exclusive inventory and should therefore overlap among all services. (Some lists differed by around one hundred names per day; we noticed that

some services removed names containing trademarks or punycode domains whereas other services did not.) We use the overlap to convert all lists into a common time convention as follows: As a preliminary reference, we use Dynadot's list, which is the only one that declares its timestamps as UTC, and is also the most complete list. Separately for each other list, we extract the dates associated with each domain found in both that list and Dynadot's list, and compute the distribution of the time difference. We use the mode of this distribution as each list's time offset from Dynadot. Once we have adjusted all lists, we observe that they agree on the same date for 99.99 % of `com` and `net` domains and around 80 % of `org` and `biz` domains, with the vast majority of disagreements involving only a one-day difference. We hypothesise that the qualitative difference between `com`/`net` and the other zones may be due to different ways of collaboration between the registries and the drop-catch services; Verisign manages both `com` and `net` and is known to make lists of pending delete domains available to registrars, whereas we could not find any public information regarding the other registries' policies. To resolve any disagreement among the lists about the deletion date of a domain, we apply a majority voting algorithm and pick the date declared by most of the lists.

3.2 Domain Status Tracking

The domain lists compiled by pre-release and drop-catch services alert us about new domains becoming available, but they do not contain the outcome, that is, whether a pre-release domain was sold to a new owner, or if a deleted domain has been re-registered. We obtain this information from the respective registry's WHOIS database, which is the official public source for domain registration metadata. Since WHOIS databases contain only current data but no history, we need to extract data periodically in order to detect changes. Furthermore, while access to WHOIS databases is public, it is also rate limited, which bounds the number of domains that we can track. We conducted two experiments, each designed to measure a specific aspect of domain re-registrations:

- pre-release sales and drop-catch re-registrations over a four-week period in 2016, our MAIN data set, and
- domain tasting in drop-catch re-registrations during one week in 2017 (TASTING).

A common principle of both experiments was that we sourced new domains from the daily lists during the *seed time*, and we periodically requested WHOIS records for these known domains during the *tracking time*.

Zone	com	net	org	biz	name
Pre-Release Domains	1.2 M	135 k	116 k	21 k	182
min/day	23.8 k	2.5 k	2.1 k	388	2
median/day	43.5 k	4.9 k	4 k	710	7
max/day	53.7 k	6.7 k	6.4 k	1.1 k	15
Sales/Late Renewals	70.6 k	5.9 k	4.8 k	475	6

Table 1: The number of domains on all pre-release lists during our 28-day measurement period along with the daily min/median/max, and total domains not deleted (either sold by platform or renewed by owner).

Zone	com	net	org	biz	name
Pending Delete Domains	2.1 M	255 k	169 k	51 k	–
min/day	61.6 k	7.4 k	4.8 k	1.2 k	–
median/day	76.4 k	9.2 k	6.1 k	1.7 k	–
max/day	92.1 k	11.2 k	7.5 k	2.6 k	–
All Observed Re-Registr.	334.3 k	33.5 k	15.5 k	3.3 k	–
"Day 0" Re-Registrations	215.6 k	16.9 k	7.9 k	0.9 k	–

Table 2: The number of domains on all pending delete lists during our 28-day measurement period along with the daily min/median/max. Note the strong daily variation. Our observations of overall re-registrations are right censored, whereas deletion day re-registrations are not.

3.2.1 MAIN: Pre-Release & Drop-Catch Domains

During a four-week period starting in late July 2016, each day we began tracking all `com`, `net`, `org`, `biz` and `name` domains appearing on the pre-release and pending delete lists mentioned above with an end date three days in the future. That is, we requested the WHOIS records of each pre-release and pending delete domain three days before the end of the auction or the deletion date, respectively. This first WHOIS lookup allowed us to extract domain metadata corresponding to the expiring registration, such as the original domain creation date, the expiration date, and any status flags corresponding to expiration states (Figure 1) that may be set, such as *pending delete*. We then repeated each lookup every 2 weeks. The frequency was chosen low enough to include every listed domain while not exhausting our limited budget of lookups, but high enough to observe transient status changes such as the 30-day *redemption period*. After the end of the four-week period, we stopped adding new domains from the lists, but we continued tracking the previous sample until mid-December. For our lookups, we respected conservative delays between queries (2 s for `com`, `net`, `biz` and `name`, and 30 s for `org`), and we were able to carry out our lookups without being blocked. Overall, we tracked more than four million domains, as shown in Table 1 for pre-release, and in Table 2 for pending delete domains.

Recall that pre-release domain sales take place during the *auto-renew grace period* so that registrars can delete the domains without incurring any cost if they do not sell. Since the length of this period is no more than 45 days, we can conclude that a sale or renewal has taken place if the WHOIS status at least 45 days after the initial lookup

shows that (1) the domain still exists, (2) the domain is not in a *redemption period* or *pending delete* state (it is not being deleted), and (3) the domain's records still have the same creation date as in the first lookup (the domain has not been re-registered). Note that we do not possess registrant information for `com` and `net` domains due to their thin WHOIS model. In these zones, registrant information is not available from the registry, but must be requested from the domain's sponsoring registrar. Prior work by Liu et al. found that registrars' Whois servers typically have much lower, and usually undisclosed rate limits, which makes it challenging to extract registrant data at scale [34]. Furthermore, the authors described a growing number of domains hiding their true ownership through privacy protection services, over 20 % in 2014. For the purposes of this work, we decided that the benefits of ownership data did not justify the effort needed to collect it. As a result, we cannot distinguish pre-release sales from domain owners using the very last opportunity to renew their expired domain, since both cases result in the domain remaining active. However, we believe that only a small fraction corresponds to last-minute renewals because registrars contact their customers many weeks before expired domains go to auction and disincentivise late renewals with higher fees, as discussed in Section 2.2.

Pending delete domains can be re-registered as soon as the domain exits the *pending delete* status. We can detect a re-registration by a creation date that is on or after the "drop date" from the pending delete lists. If a domain is re-registered on the same day that the previous registration was deleted, we call it a *0-day* drop-catch re-registration.

3.2.2 TASTING: Drop-Catch Domain Tasting

Domain tasting registrations are active for a maximum of five days, the duration of the *add grace period*, before they are deleted. Since the two-week measurement frequency in the MAIN data set cannot reliably find every instance of tasting registrations, we discarded any such observation from that data set to retain only "surviving" registrations, and we designed a separate experiment to measure tasting. Specifically, for the TASTING experiment's seed time of one week in late January 2017, we extracted Whois records for all domains from the pending delete lists three times at fixed delays: Three days before the deletion date to observe the registration instance that was about to be deleted, one day after the deletion date to observe any drop-catch re-registration, including short-lived tasting registrations, and six days after the deletion date to find out whether a drop-catch re-registration had been cancelled (due to tasting) or remained active.

Zone	com	net	org	biz	name
Total Domains (Aug'16)	131 M	16.1 M	11.3 M	2.3 M	166 k
added (per day)	81.3 k	8.7 k	5.4 k	1.3 k	26
deleted (per day)	72.7 k	8.8 k	6.5 k	1.5 k	66
"Day 0" Re-Reg. Adds	9.5 %	7.0 %	5.2 %	2.4 %	–
(mean, per day)	7.7 k	605	280	32	–

Table 3: The total number of domains registered in August 2016 as well as the daily mean of domains added and deleted in July and August 2016 according to the ICANN registry reports. Deletion day re-registrations (as determined in our measurements) are given both in absolute terms and as a fraction of daily domain creations. They represent an upper bound on successful drop-catch domain creations.

3.3 Limitations

Our analysis relies on domain lists to discover expiring and deleting domains. While the high overlap among pending delete lists of competing services makes us confident that their union represents all `com`, `net`, `org` and `biz` domains that are about to be deleted, our pre-release lists do not cover the full inventory of expiring domains available for purchase due to the fragmented ecosystem. However, we believe that our pre-release lists cover a majority of the available inventory as we source our data from the most popular platforms. According to our results in Section 4.1, the vast majority of domains on pre-release lists is not sold but deleted, which causes those domains to ultimately appear on pending delete lists. Our pre-release lists are more than half the size of the pending delete lists, with the largest part of the difference likely due to registrars that do not offer any pre-release sales at all.

This paper analyses ownership transfers of expiring or deleted domains, which implies a bias towards domains of lesser value. Highly valuable domain names are likely to be sold directly rather than expiring due to non-renewal.

4 Analysis

We begin our analysis by providing context for expiring domains. According to ICANN's registry reports, 2.2 M `com` domains were deleted in August 2016, which corresponds to 1.7 % of all registered `com` domains, as shown in Table 3. In contrast, about 2.6 M `com` domains were added during the same period, hinting at a constant and sizeable turnover in registered domains. While some of the added domains were never registered before, many are re-registrations of old domains. In this paper, we focus on *drop-catch* domains that are re-registered on *day 0*, that is, on the deletion day of the old registration.

Some expired domains may be available even before they are deleted, and our pre-release lists (Table 1) advertise around 1.2 M `com` domains over a period of 28 days. The large number of expiring domains that can be acquired by means of an ownership transfer instead of a

Zone	com	net	org	biz	name
Dynadot	17.1 %	32.9 %	13.7 %	22.4 %	27.8 %
	1.9 k	607	176	17	5
GoDaddy	5.31 %	3.33 %	4.06 %	2.21 %	0.65 %
	30.5 k	1.9 k	2.0 k	164	1
NameJet	9.89 %	7.63 %	6.81 %	4.84 %	–
	27.1 k	2.4 k	1.5 k	134	–
SnapNames	3.39 %	2.41 %	2.59 %	1.57 %	–
	11.1 k	981	1.1 k	160	–

Table 4: Pre-release domains not deleted (likely sold) per platform.

re-registration illustrates that security mechanisms should avoid relying exclusively on creation-time features to detect potential ownership changes. To conclude this overview, Table 2 shows that the number of domains on pending delete lists supplied by drop-catch services is in line with the official statistics from the ICANN reports. Therefore, we can rely on these pending delete lists to discover the domains that are about to be deleted.

4.1 Demand for Expired Domains

Using the predicted deletion dates from the pending delete lists (in the MAIN data set), we find that 10.1 % of all deleted `com` domains are re-registered on the same day, that is, the earliest possible day for a re-registration. Smaller zones also exhibit smaller fractions of same-day re-registration at 6.6 % of `net`, 4.7 % of `org` and 1.8 % of `biz`. Our results suggest that re-registrations are not only a common phenomenon in general, but also one driven by enough competition to cause re-registrations to happen as early as possible. The deletion day has the highest daily rate of re-registrations. For instance, after the 10.1 % on the deletion day, it takes about one month until the next 5 % of deleted `com` domains are re-registered.

Given that many buyers appear to be interested in gaining access to a domain name as soon as possible, we look at the sales of pre-release domains, which are available even before they are deleted. Pre-release domains are typically exclusive inventory of the selling platform, thus competition among prospective buyers would play out monetarily in auctions as opposed to a timing-based technical arms race between competing services.

The four pre-release domain lists that we use in our research are slightly different in nature. GoDaddy and Dynadot are domain registrars themselves and likely sell only their own customers' expired domains—all `com` domains on these two lists were initially registered by only 16 and 11 different registrar IDs, respectively. NameJet and SnapNames, on the other hand, appear to be marketplaces with a number of collaborating registrars; we observed 277 and 263 registrar IDs in their `com` domains.

Taken together, the four pre-release lists contain more than half as many domains as the pending delete lists during the same time span in the `com`, `net`, and `org` zones, and less than half for `biz`. While pre-release lists are biased towards participating registrars, and only domains not sold during the pre-release phase ultimately appear on a pending delete list, the pre-release domains available through the four services make up a sizeable portion of the entire expiring domain inventory. It is worth investigating how many of them are sold pre-release instead of becoming available as pending delete domains.

Since purchases of pre-release domains are guaranteed and the prices sometimes lower than drop-catch re-registrations, one might expect to observe a higher fraction of pre-release sales than drop-catch re-registrations. However, the numbers in Table 4 do not support such a general trend. In nearly all zones, Dynadot and NameJet sell a larger fraction of their inventory than the corresponding re-registration rates one month after deletion. GoDaddy and SnapNames, on the other hand, sell a considerably lesser fraction—GoDaddy has the largest inventory of domains but sells only 5.31 % of their pre-release `com` domains, which is half the percentage of overall `com` drop-catch re-registrations on the deletion day.

Pre-release domains that are not sold are marked for deletion and will appear on pending delete lists. While one may suspect that the availability of pre-release domains of a registrar might have a negative affect on drop-catch re-registrations, we did not find any clear difference in re-registration rates of registrars that offer pre-release domains compared to others that do not. In fact, we observed a surprisingly frequent phenomenon of pre-release domains that were not sold initially, but re-registered as drop-catch domains once they had been deleted.

4.2 Competitiveness of Re-Registrations

To gain a better understanding of how domains are re-registered on their deletion day (and verify the third-party accounts cited in Section 2.3), we need a fine-grained view of the creation time of the re-registration. Unfortunately, WHOIS records for `com` and `net` domains do not contain the exact time when the domain was created, but for `org` and `biz`, we can plot domain creations with a second precision. Figure 3 shows the UTC time-of-day creation time of all `org` and `biz` re-registrations from the pending delete lists separately for the deletion day, that is, drop-catch re-registrations, and all re-registrations that happened on a later day. Re-registrations on any day after the deletion day are relatively evenly distributed over the day with no strong time-of-day effect. Re-registrations on the deletion day, however, do not begin until 14:30 for `org` and 17:00 for `biz` with around 90 % and 60 % of all re-registrations on that day occurring within the first 30 minutes. The remaining re-registrations during the remaining time of the day are again evenly distributed. This

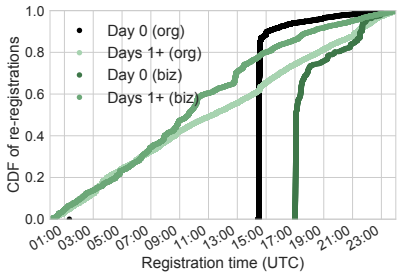

Figure 3: CDF of the time of day when domains from pending-delete lists are re-registered, separately for day 0 (drop-catch) and any later day. Drop-catch re-registrations occur in a spike after deletion of the domains, whereas regular re-registration times are more evenly distributed.

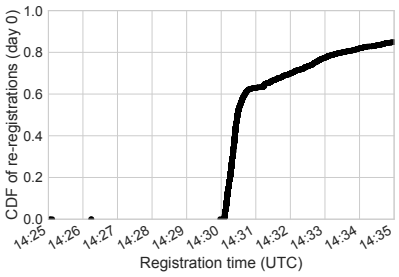

Figure 4: CDF of re-registration times for `org` on day 0 (minute-level detail of Figure 3). Except for a few outliers, re-registrations begin at 14:30 and slow down before 14:31 UTC, at which point more than 60 % of the deletion day re-registrations have already occured.

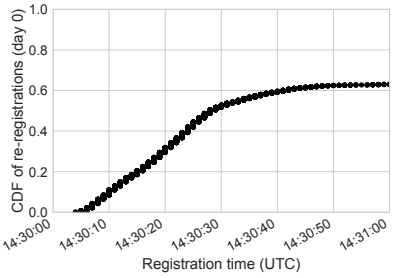

Figure 5: CDF of re-registration times for `org` on day 0 (second-level detail of Figure 4). More than half of the deletion day re-registrations occur within the first 30 s; only around 10 % are re-registered during the following 30 s.

suggests that the drop process of `org` and `biz` is similar to the one reported for `com` and `net`. In other words, all domains scheduled to become available for re-registration on a given day do so within a brief "drop" interval.

Figure 4 contains a minute-precision detail of the same plot for `org` re-registrations on day 0 and shows that over 60 % of the day's re-registrations occur in the minute between 14:30 and 14:31. Figure 5 zooms in even further to a second-level precision and reveals that more than half of the day's re-registrations occur within the first half of the first minute; only around 10 % are re-registered during the following 30 s. The high density of re-registrations during a very short time period hints at how competitive the re-registration race is. For instance, manual attempts to re-register a sought-after domain on its deletion day rather than paying for a drop-catch service will likely fail.

Re-registrations on day 0 for `biz` are significantly slower than `org`, with about 50 % in the first five-minute interval and roughly 20 % during the next 30 minutes. The lower re-registration speed may be an indicator for lower interest in `biz` re-registrations. In fact, `biz` is the smallest of the four zones with pending delete domains analysed in this paper, and it is decreasing in size (Table 3).

To further investigate how many resources are dedicated to re-registrations, we compare the number of registrar IANA IDs used for re-registrations on day 0 as opposed to any later day. Registrar IDs are used in WHOIS records to identify the sponsoring registrar of a domain, but there is no 1:1 mapping to companies since a registrar could use multiple IDs (e.g., due to acquisitions of other registrars), and it has been reported that drop-catch services use multiple credentials in order to increase their success rate during the drop [8, 28]. Indeed, we find that re-registrations of `com`, `net` and `org` domains on day 0 are carried out with a very large diversity of registrar IDs. For instance, we observed a total of 1,745 registrar IDs for `com` 0-day domains, but only 308 registrar IDs for `com` re-registrations on any later day combined. Re-registrations of `net` and `org` similarly use many times more registrar IDs on day 0 as opposed to the entire period after the deletion day. At the same time, re-registrations on day 0 only account for between half and two thirds of all observed re-registrations. This illustrates that disproportionately more resources are utilised for 0-day re-registrations. Consider, for instance, that the 1,745 registrar IDs correspond to a daily median of only 7.7 k `com` 0-day re-registrations. For `biz`, the trend is inverse with only `34` registrar IDs used on the deletion day compared to `94` afterwards; this is another indicator that the `biz` drop is less competitive.

The higher number of registrar IDs in use for deletion-day re-registrations goes in hand with a much lower skew towards the most active IDs. According to Figure 6, the 10 most active registrar IDs on the deletion day account for only 20 % of same-day re-registrations. While the 90 next registrar IDs together hold the same market share, there is significant weight in the middle ranks as half of the registrar IDs (ranks 100 – 1000) account for over half of deletion-day re-registrations. This effect cannot be observed at all for re-registrations after the deletion day (Figure 7), where the top 10 registrar IDs alone account for almost three quarters of re-registrations. The more equal distribution of deletion-day re-registrations over registrar IDs suggests a tight competition where the top performers hold a small but not overwhelming advantage.

The high number of registrar IDs on the deletion day is centred around the time of the drop, as illustrated in Figure 8. Within the first 30 s after the drop, hundreds of registrar IDs are being used each second, but after around 15 minutes this number already decreases to fewer than 10 registrar IDs per minute. This suggests that the 0-day distribution in Figure 6 is dominated by the drop, and that the remainder of the day may be more akin to the post-deletion day distribution in Figure 7, with the additional resources being deployed only for the time of the drop.

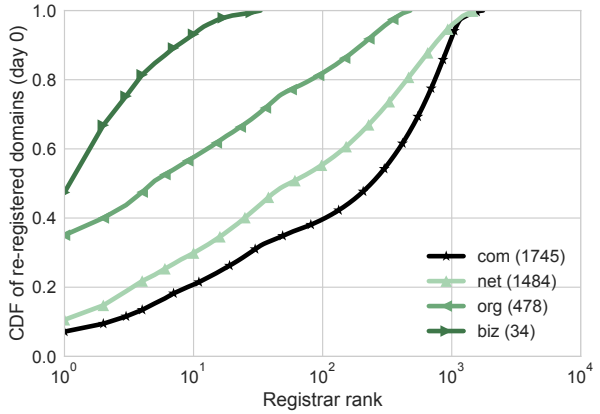

Figure 6: CDF of deletion day domain re-registrations per registrar ID ranked by re-registration volume (log scale). The 10 most active registrar IDs are responsible for 20 % of `com` re-registrations on day 0.

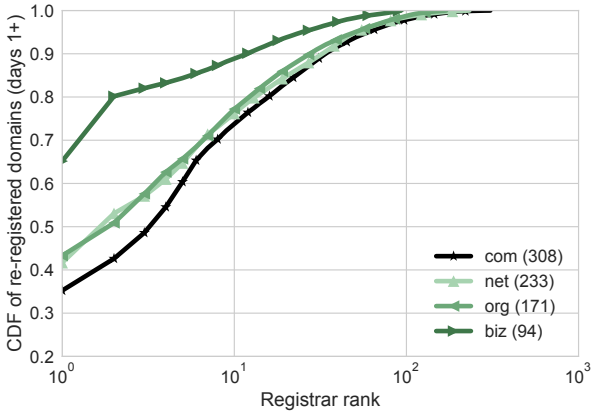

Figure 7: CDF of domain re-registrations *after* the deletion day per registrar ID ranked by re-registration volume (log scale). The 10 most active registrar IDs account for 74 % of `com` re-registrations on days 1+.

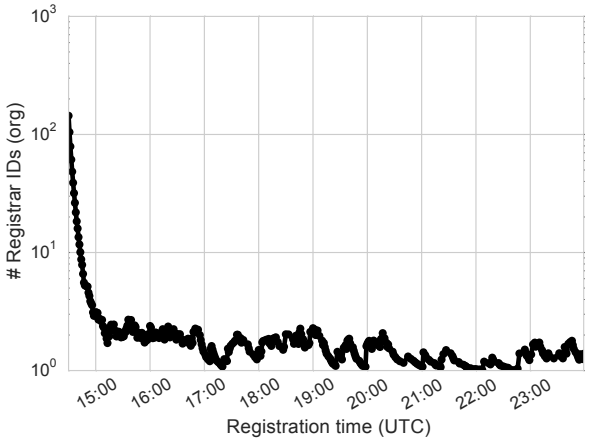

Figure 8: Histogram of distinct registrar IDs observed for `org` re-registrations during one-minute intervals on the deletion day (log scale). The number rapidly decreases from hundreds of registrar IDs used directly after the drop to just a few per minute half an hour later.

4.3 Drop-Catch Registrar Characteristics

We now show that the characteristics of registrars engaging in drop-catch re-registrations can be very different from regular registrars. To that end, we compute metrics from ICANN's registry transaction report for `com` in August 2016 and make the following observations:

- Domain creations by drop-catch registrars are typically for a one-year duration, whereas other registrars often have a higher fraction of domains paid in advance for up to ten years. For example, 30.8 % of domain creations by GoDaddy's registrar 146 were for two or more years, whereas the drop-catch registrars 627 (Pheenix), 635 (SnapNames) and 1570 (DropCatch) created only one-year registrations. This suggests a lower willingness of up-front investments to commit to domain names in the long term.
- Drop-catch registrars are rarely on the receiving end of domain transfers between registrars, as most transfers are away to another registrar. For the regular registrars OVH (433), Gandi (81) and GoDaddy, 27.6 %, 35.8 % and 55.7 % of all domain transfers were outbound, whereas the percentage was 100 % for Pheenix and SnapNames. These registrar IDs appear to be used for creations of drop-catch domains, but not for management of regular domains.
- The success ratio of attempted domain creations is very low for drop-catch registrars, with a large majority of domain creations failing. The sample registrar IDs of Pheenix and DropCatch had success rates of 0.05 % whereas GoDaddy's success ratio was 71.7 % and Gandi's was 99.3 %. This confirms accounts of the drop, when the registry systems are flooded with speculative domain creation requests, most of which fail because the domain is not yet available, or has already been re-registered by a competitor.

Especially the latter point has implications for the domain registration systems managed by the registries. In August 2016, more than 99.9 % of all attempted domain creations in the `com` zone failed. Conservatively estimated, at least 80 % of all attempts can be attributed to failed drop-catching, which means that drop-catch services are responsible for a very large majority of all domain creation requests received by Verisign, the `com` registry.

The large number of registrar IDs engaging in drop-catch found in Section 4.2 does not correspond to thousands of independent drop-catch services, but rather some drop-catch services using large numbers of registrar IDs. To better characterise the drop-catch ecosystem, we need to find out which registrar IDs collaborate and which ones compete. To that end, we group the individual registrar IDs found on the complete IANA list in February

	Name	IDs	%
1	DropCatch.com	1252	42.6 %
2	Pheenix.com	498	16.9 %
3	SnapNames.com	466	15.8 %
4	LogicBoxes.com	53	1.8 %
5	MyDomain.com	43	1.5 %
6	XZ.com	21	0.7 %
7	Name.com	19	0.6 %
8	Dynadot.com	19	0.6 %
9	22.cn	16	0.5 %
(total)		2387	81.1 %

Table 5: All clusters with more than 10 registrar IDs as of Feb. 2017. The Top 3, all drop-catch services, control 75 % of accredited registrars.

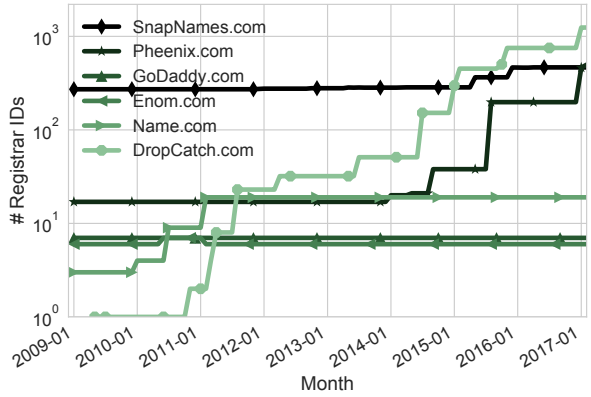

Figure 9: Historical perspective on cluster size in terms of registrar IDs, from ICANN `com` reports until February 2017. Drop-catch services increased their size, whereas regular registrar clusters remained constant.

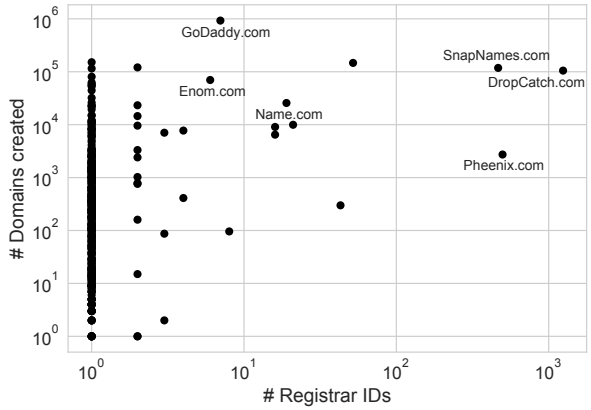

Figure 10: Cluster size vs. domain creations in February 2017. Regular registrars such as GoDaddy or Enom have high numbers of total creations using very few registrar IDs, whereas drop-catch services such as SnapNames or DropCatch have an order of magnitude fewer domain creations but use almost two orders of magnitude more registrar IDs.

2017 into clusters likely belonging to the same company when they share the same official contact email address or phone number, or if their name differs only by a number. For instance, the list contains 1,201 IDs with names "DropCatch.com *n* LLC", where *n* is a number. Another cluster contains names that look similar to the human eye, such as "Charlemagne 888, LLC," "George Washington 888, LLC," and "Napoleon Bonaparte, LLC"—these are grouped because of their contact information and belong to the drop-catch service Pheenix. Almost 92 % of the clusters consist of a single registrar ID, but a small number of clusters is very large. Table 5 shows all nine clusters with more than ten registrar IDs. Their sizes correspond to what was previously reported by specialised online media [38, 39]. Overall, the clusters comprising more than ten registrar IDs account for more than 81 % of all registrar IDs on the IANA list, and the Top 3, all drop-catch services, account for three quarters of all accredited registrars. (In contrast, as shown in Table 3, drop-catch services do not register such a large share of domains—at most 9.5 % of successful `com` domain creations each day can be attributed to drop-catch re-registrations.) Note that our clustering groups only registrars with evident similarities in their names or contact information. Some drop-catch services are said to have agreements with independent registrars to use their credentials for the duration of the drop. Therefore, these clusters likely underestimate the true "horse power" of drop-catch services.

To gain a historical perspective, we search ICANN's registry transaction reports for the first time a registrar ID has been observed to register domains (in the `com` zone). Figure 9 shows that regular domain registrars such as GoDaddy maintain a constant or only modestly increasing number of registrar IDs, whereas drop-catch clusters grow over two orders of magnitude in an apparent arms race among drop-catch services [38, 39]. Note that the plot only shows cluster size increases due to newly allocated registrar IDs because we always apply the February 2017 clustering. As a result, initially independent registrars that were later acquired and became part of a larger cluster are shown as part of that cluster from the beginning.

It is important to keep in mind that maintaining a large number of registrar IDs is not at all necessary in order to register large numbers of domains. Figure 10 plots all clusters in terms of the number of domains registered in February 2017, and the number of active registrar IDs of the cluster in the same month. GoDaddy registered by far the most domains, but used fewer than ten registrar IDs. Drop-catch services such as SnapNames or DropCatch, on the other hand, used large numbers of registrar IDs to re-register relatively few domains. According to ICANN, maintaining a registrar ID costs more than USD 4,000 in yearly fees alone [25], which amounts to several million dollars per year for the largest clusters. This suggests that controlling a large number of registrar IDs is considered a prerequisite to success in the competitive drop-catch business—but it also suggests that drop-catch services expect the generated revenue to justify the investment.

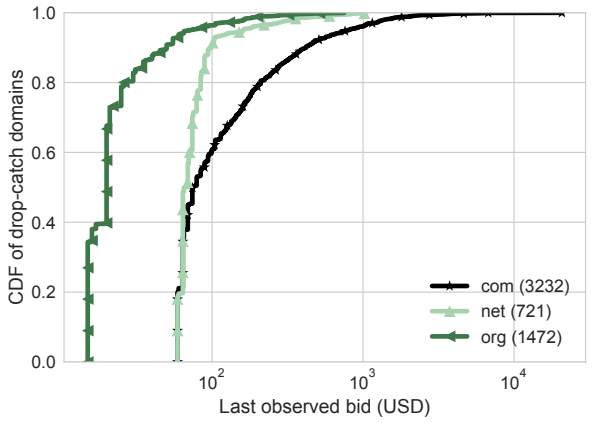

Figure 11: CDF of the last observed bids for successfully acquired drop-catch domains with multiple backorders on DropCatch (February to June 2017). Most auctions remain close to the starting price, whereas a few exceed one thousand US dollars. The curve for `org` is shifted to the left because of a promotion ($ 15 starting price instead of $ 59).

4.4 Value and Use of Drop-Catch Domains

As of 2017, a regular `com` registration costs around $ 15 per year; a drop-catch re-registration can cost $ 60 to $ 80. When multiple customers backorder the same domain, the winner is usually determined in a three-day private auction. DropCatch, however, conducts these auctions in public. We extracted the current bid around 3.5 hours before the end of each auction during five months in early 2017. Figure 11 shows that a majority of auctions remained close to the starting price, whereas 3.9 % of `com` auctions exceeded one thousand dollars. Overall, DropCatch successfully re-registered an average of 2773 `com` domains per day in early 2017 (Table 6). It appears that only a small fraction of those domains received backorders by multiple interested customers, as the median number of auctions was 21 per day for `com`, 5 for `net`, and 10 for `org` (the latter likely due to an ongoing promotion). Our observation 3.5 hours before the end only allows us to give an approximate lower bound on the daily auction revenue with a median of $ 4108 for `com`, $ 382 for `net` and $ 254 for `org`. Based on a starting price of $ 59, the `com` drop-catch domains sold without an auction yielded an estimated daily revenue of $ 162 k. In comparison, the 1252 registrar IDs controlled by DropCatch represent a daily fixed cost of at least $ 13.7 k, or approximately $ 5 per sold `com` domain (ignoring other costs and domains).

Pre-release sales, in contrast, are carried out at comparatively minor cost to the registrars since they already manage the domain and can return it to the registry without any fee if it is not sold during the grace period. The pre-release lists often contain metadata about the current auction state of each domain, such as the number of bidders and the current price. Unfortunately, the data does not refer to when the auction ended, but to when the list was compiled by the service the morning or night before. Since auctions tend to be busiest just before they conclude, our data does not allow us to characterise the final prices of pre-release sales. Instead, we use it to investigate how early customers start bidding on expiring domains.

Surprisingly, at our latest observation point, nearly all ultimately sold pre-release domains are still at the starting price. For instance, only 8.9 % of Dynadot's sold `com` domains have an observed price higher than the starting price. However, there are some outliers, such as a GoDaddy `com` domain listed at $ 64,888. The relatively low proportion of sold domains along with auctions that are still inactive on the day before a domain is sold suggest a lower competition among buyers of pre-release domains compared to drop-catch domains.

From a buyer's perspective, certain premium-priced pre-release and drop-catch domains must appear more attractive than regularly-priced domains that are freely available for registration. The desirability of a name is difficult to measure. Therefore, we focus on two metrics that relate directly or indirectly to the number of visitors that a domain is expected to receive due to its past history.

Drop-catch re-registrations appear to be correlated to the traffic data reported by the pending delete lists, as over 80 % of `com` domains with more than 100 k visitors are re-registered on the deletion day as opposed to 50 % of domains with 10 k – 100 k visitors, or 5 % of domains with fewer than 1 k reported visitors. We observe a similar trend for the age of the domain, with those that had been registered for a longer time period being more likely to be re-registered immediately after deletion. This phenomenon is in line with our prior findings [29].

Similarly to drop-catch domains, pre-release domains that are reported to receive more traffic or that have already been registered for longer time spans are more likely to be sold than other domains. For instance, Dynadot and GoDaddy `com` domains that were sold had a median registration length of four years as opposed to one year for Dynadot's `com` domains that were not sold as pre-release (GoDaddy: 2 years). A long registration period however does not guarantee that a domain will be sold, as we observed GoDaddy domains over 20 years old in both the sold and not sold categories.

To provide a first cursory overview of what re-registered websites are being used for, we conduct a small-scale manual classification of websites. We inspect a random sample of 50 drop-catch domains six months after the re-registration, and find that 23 are parked and display a "for sale" message or textual advertising; nine sites contain advertising for online casinos, one is malicious, two are empty, and eight cannot not be loaded due to an error. Even though just a superficial analysis, it appears that only a small minority of the re-registered

sites contain any useful content, while a majority attempt to monetise incoming traffic in a rather generic way. We are planning to further explore this topic in future work, and focus this paper on *how* domains are re-registered.

4.5 Comparison of Drop-Catch Services

To better compare the relative performance of drop-catch services, we rank the most active clusters of registrar IDs according to com re-registrations on the deletion day (Table 6). In 2016, DropCatch dominated the ranking with more than twice as many drop-catch re-registrations as SnapNames, the cluster ranked second.

Due to a lack of visibility into registration times, we cannot distinguish between domains re-registered *during* the drop and those that were still re-registered on the deletion day, but *after* the drop. GoDaddy, for instance, is ranked fourth in deletion day re-registrations in 2016. While GoDaddy does accept domain backorders, it is unlikely that all 11 k deletion-day re-registrations occurred during the competitive drop, given that the GoDaddy cluster consists of only seven registrar IDs. It is more likely that these domains were re-registered after the drop, and their relatively large number may be due to GoDaddy's position as the most popular domain registrar overall. Similarly, in 2017, the Alibaba cluster with only two registrar IDs is ranked first, before the DropCatch cluster with 1252 registrar IDs. Indeed, certain domain name speculators appear to leverage reseller APIs to re-register domains on the deletion day (e.g., using desktop software [41]). While the cost is comparable to regular domain registrations, such "do-it-yourself" drop-catching is expected to succeed only for relatively non-competitive domains not targeted by the large drop-catch services.

The relative ranking of the known drop-catch services DropCatch, SnapNames and Pheenix remains the same in our 2016 and 2017 data. An interesting observation is that Pheenix added 300 registrar IDs in late 2016 [39] and controlled more registrar IDs than SnapNames during our 2017 measurement. However, Pheenix is ranked only eleventh with 301 re-registrations, as opposed to SnapNames with 7623 on rank three. Even before the increase, Pheenix re-registered fewer domains per registrar ID than DropCatch or SnapNames, suggesting that Pheenix may be less efficient in using their registrar IDs.

Despite the widely supported recommendation that customers place backorders with all services [7, 12, 31], we do not know how many customers follow this advice, thus our findings should not be seen as a comparison of how *successful* drop-catch services are in fulfilling their customers' orders. Furthermore, our clustering cannot group registrar IDs that collaborate during the drop without exhibiting any clear administrative relationship. For some of the clusters, we could not find any public information

	2016 (4 weeks)		**2017** (1 week)	
1	DropCatch.com	87437	Aliyun.com	20208
2	SnapNames.com	40552	DropCatch.com	19411
3	XZ.com	20104	SnapNames.com	7623
4	West.cn	8854	LogicBoxes.com	2201
5	GoDaddy.com	7389	Onamae.com	1069
6	Onamae.com	6573	XZ.com	875
7	DNS.cn	4935	GoDaddy.com	875
8	BizCN.com	4553	West.cn	808
9	Oray.com	4031	BizCN.com	432
10	CNDNS.com	3200	OpenSRS.com	384

Table 6: The Top 10 clusters according to deletion-day re-registrations of com in 2016 and 2017 (MAIN and TASTING data sets, respectively). There is some variation between the years, and the deletion-day rankings are very different from general domain name registrations (not shown).

regarding a drop-catch service that might be operated by the same corporate entity. At the same time, some well-known drop-catch services such as Pool are not among the most highly ranked clusters, which leads us to believe that we cannot currently characterise their performance due to the limitations inherent in our methodology.

4.6 Domain Tasting

ICANN considers domain tasting a "profit-making abuse of the domain name system" [26] and discourages it by allowing each registrar only a limited number of free domain deletions during the initial five-day *add grace period* after domain creation. Traditionally, domain tasting has been understood as a way for the domain registrant to test how much traffic the domain receives before deciding whether to keep or return it (e.g., [6]). However, we show that domain tasting can also be used for a similar purpose as the *auto-renew grace period* in the case of pre-release domain sales. That is, a service can use the *add grace period* to attempt selling a domain to a customer and return it to the registry for free if no sale is made.

The restrictions imposed by ICANN affect only registrars with a high ratio of domain deletions per registrar ID. Drop-catch services, however, already need to maintain a high number of registrar IDs in order to compete in the drop. In absolute terms, they could delete a high number of domains for free while staying below ICANN's thresholds on a per-registrar ID basis. We designed the TASTING experiment to specifically measure domain tasting among domains re-registered on the deletion day of the prior registration. We find that domain tasting is relatively uncommon. Only about 2.1 % of com domains re-registered on the deletion date (and much fewer in the other zones) are deleted within the first five days. However, we find that SnapNames is responsible for over 98 % of all domain tasting among drop-catch domains. Upon closer inspection, we find that SnapNames' website features a file of domain names "in auction," which appears to contain only domain names that were recently

re-registered during the drop, and that all have an active website with a parking page during the three-day duration of the auction. When checking the registration status of these domains a week later, we find that 41.2 % of the domains have been deleted. We suspect that SnapNames proactively registers domain names during the drop, even without having received a specific backorder from a customer, and deletes these names if they do not find a buyer.

4.7 Summary

- Domain ownership can change fast, and often: 10 % of `com`, and 5 % of `org` domains are re-registered on the same day as the old registration is deleted. *Domain-based trust mechanisms should anticipate ownership changes as a common, expected event.*
- Pre-release sales allow ownership changes without implication of the prior owner and maintain the old registration: Expired domains as old as 20 years are available with comparatively little competition. *Anti-abuse tools may need improved detection of ownership changes that are not re-registrations.*
- Drop-catch services have a significant impact on the domain name registration system: The Top 3 account for 75 % of all accredited registrars, and drop-catch is responsible for over 80 % of *all* domain creation attempts, yet results in no more than 9.5 % of successful `com` domain registrations. *Drop-catch consumes a disproportionate share of resources.*
- Drop-catch re-registrations are highly competitive: Half of `org`'s same-day re-registrations occur within 30 s of the drop (`biz`: within 5 min of the drop), and 0-day re-registrations have the highest diversity and most evenly distributed market share of registrar IDs. *High demand for certain expired domains and the willingness to pay premium prices sustain an entire industry dedicated to "recycling" old domains.*
- Only few drop-catch domains are put to "good" use: Most seem to contain nothing but advertisements and parking pages to profit from residual traffic. *Many if not most drop-catch re-registrations may be of limited value to the Internet community as a whole.*

5 Discussion & Conclusions

Our analysis has shown that there is significant demand for expired domain names (e.g., over 10 % of all `com` domains re-registered immediately on the day that they were deleted), and that there is a highly competitive environment of drop-catch services that race to be the first to re-register a domain in the very instant that it is deleted (e.g., over half of `org` re-registrations on the deletion day take place within a 30 s time frame). In the current system, the drop-catch service with most technical resources and the best insight into details of the drop is going to be most successful in re-registering deleted domains for their customers. However, the uncertainty of this process and lack of transparency as to which service is most successful result in the common recommendation that customers place orders with all services [7, 12, 31]. The re-registration race is open to all registrars, and manual re-registration is at least a theoretical possibility, but it is quite wasteful of resources as drop-catch services cause a daily flood of requests as a byproduct of determining the next owner.

Pre-release domain sales typically take place as auctions, thus they are efficient from a technical point of view. However, there are administrative concerns, as pre-release sales do not allow buyers to freely choose their registrar, prevent the former domain owner from using the 30-day *redemption period* to recover the expired domain, and might incentivise registrars to make late domain renewals more difficult (or expensive) for their customers because of the potentially more lucrative pre-release sales.

From a security perspective, domain ownership changes are problematic because of their potential to break domain-based trust mechanisms [44], abuse residual trust [33], and more generally profit from residual traffic in various ways that are not necessarily illegal, but often undesirable. While banning domain ownership changes altogether may not be practicable, we argue that the process should be made more transparent. State-of-the-art anti-abuse systems may find it challenging to detect domain ownership changes such as pre-release sales because they do not result in a new domain creation. As a policy-based approach, registrars could be required to maintain a public log of ownership changes, similar to Certificate Transparency [30], so that security mechanisms can "reset" trust in a reliable way: Whitelists can drop domains after certain changes of ownership, web browsers can purge cached website permissions, and websites can remove links pointing to a deleted domain.

What exactly drives that demand for expired domain names, whether it is intended "productive" use, abuse [22, 33], monetisation through advertising [48], or speculation with the goal of reselling the domain name, is still an open question, and an interesting direction for future work.

Acknowledgements

The authors would like to thank Farsight Security and Manuel Egele for providing valuable database access and computing resources to carry out the measurements.

References

[1] AGTEN, P., JOOSEN, W., PIESSENS, F., AND NIKIFORAKIS, N. Seven Months' Worth of Mistakes: A Longitudinal Study of

Typosquatting Abuse. In *Network and Distributed System Security Symposium* (2015).

[2] ALRWAIS, S., YUAN, K., ALOWAISHEQ, E., LI, Z., AND WANG, X. Understanding the Dark Side of Domain Parking. In *USENIX Security Symposium* (2014).

[3] BACKORDERZONE. Namepal Backorders. https://www.backorderzone.com/pending/download/#advanced.

[4] BACKORDERZONE. BackorderZone.com is for Sale. https://web.archive.org/web/20160527215205/http://www.backorderzone.com/for-sale.html, 2016.

[5] CHACHRA, N., MCCOY, D., SAVAGE, S., AND VOELKER, G. M. Empirically Characterizing Domain Abuse and the Revenue Impact of Blacklisting. In *Workshop on the Economics of Information Security* (2014).

[6] COULL, S. E., WHITE, A. M., YEN, T., MONROSE, F., AND REITER, M. K. Understanding Domain Registration Abuses. *Computers and Security 31*, 7 (2012), 806–815.

[7] CYGER, M. List of Domain Name Backorder Services. http://www.domainsherpa.com/domain-name-backorder-services/, 2013.

[8] CYGER, M. A Drop Catching Programming Expert Discusses the Domain Name Expiration Process - With Chris Ambler. http://www.domainsherpa.com/wp-content/pdf/Chris-Ambler-Expiration-on-DomainSherpa.pdf, 2016.

[9] DOMAIN GRAVEYARD. http://domaingraveyard.com/.

[10] DOMAINMONSTER. Expired Domains. https://www.domainmonster.com/expired-domains/.

[11] DROPCATCH. Download Center. https://www.dropcatch.com/DownloadCenter.

[12] DROPCATCH. FAQs – Should I place orders with DropCatch.com as well as other drop catch services? https://www.dropcatch.com/HowItWorks/Faq#orderswithothers.

[13] DROPCATCH. How it Works: Daily Drop Overview. https://www.dropcatch.com/HowItWorks/Overview.

[14] DYNADOT. Domain Backorders. https://www.dynadot.com/market/backorder/.

[15] GANDI.NET. Renewal, restoration, and deletion times. https://wiki.gandi.net/en/domains/renew#renewal_restoration_and_deletion_times.

[16] GODADDY. Auctions. https://auctions.godaddy.com/?countryview=1.

[17] GODADDY. What happens after domain names expire? https://www.godaddy.com/help/what-happens-after-domain-names-expire-6700.

[18] HALVORSON, T., DER, M. F., FOSTER, I., SAVAGE, S., SAUL, L. K., AND VOELKER, G. M. From .academy to .zone: An Analysis of the New TLD Land Rush. In *ACM Internet Measurement Conference* (2015).

[19] HALVORSON, T., LEVCHENKO, K., SAVAGE, S., AND VOELKER, G. M. XXXtortion? Inferring Registration Intent in the .XXX TLD. In *World Wide Web Conference* (2014).

[20] HALVORSON, T., SZURDI, J., MAIER, G., FELEGYHÁZI, M., KREIBICH, C., WEAVER, N., LEVCHENKO, K., AND PAXSON, V. The BIZ Top-Level Domain: Ten Years Later. In *Passive and Active Measurement Conference* (2012).

[21] HAO, S., KANTCHELIAN, A., MILLER, B., PAXSON, V., AND FEAMSTER, N. PREDATOR: Proactive Recognition and Elimination of Domain Abuse at Time-Of-Registration. In *ACM Conference on Computer and Communications Security* (2016).

[22] HAO, S., THOMAS, M., PAXSON, V., FEAMSTER, N., KREIBICH, C., GRIER, C., AND HOLLENBECK, S. Understanding the Domain Registration Behavior of Spammers. In *ACM Internet Measurement Conference* (2013).

[23] IANA. Registrar IDs. https://www.iana.org/assignments/registrar-ids/registrar-ids.xhtml.

[24] ICANN. Monthly Registry Reports. https://www.icann.org/resources/pages/registry-reports.

[25] ICANN. Registrar Accreditation: Financial Considerations. https://www.icann.org/resources/pages/financials-55-2012-02-25-en.

[26] ICANN. The End of Domain Tasting — AGP Deletes Decrease 99.7%. https://www.icann.org/news/announcement-2009-08-12-en, 2009.

[27] ICANN. The End of Domain Tasting — Status Report on AGP (Add Grace Period) Measures. https://www.icann.org/resources/pages/agp-status-report-2009-08-12-en, 2009.

[28] JACKSON, R. Inside a Drop Catcher's War Room: How Enom Arms Maker Chris Ambler Is Turning The Tide for Club Drop. http://www.dnjournal.com/columns/cover080504.htm, 2004.

[29] LAUINGER, T., ONARLIOGLU, K., CHAABANE, A., ROBERTSON, W., AND KIRDA, E. WHOIS Lost in Translation: (Mis)Understanding Domain Name Expiration and Re-Registration. In *ACM Internet Measurement Conference* (2016).

[30] LAURIE, B., LANGLEY, A., AND KASPER, E. RFC 6962: Certificate Transparency. https://tools.ietf.org/html/rfc6962.

[31] LEIGHTON, T. SnapNames Domain News and Views: Best Practices for Getting Names on the Drop. http://domains.snapnames.com/2016/03/25/best-practices-for-getting-names-on-the-drop/, 2016.

[32] LEVCHENKO, K., PITSILLIDIS, A., CHACHRA, N., ENRIGHT, B., FELEGYHÁZI, M., GRIER, C., HALVORSON, T., KANICH, C., KREIBICH, C., LIU, H., MCCOY, D., WEAVER, N., PAXSON, V., VOELKER, G. M., AND SAVAGE, S. Click Trajectories: End-to-End Analysis of the Spam Value Chain. In *IEEE Symposium on Security and Privacy* (2011).

[33] LEVER, C., WALLS, R. J., NADJI, Y., DAGON, D., MCDANIEL, P., AND ANTONAKAKIS, M. Domain-Z: 28 Registrations Later – Measuring the Exploitation of Residual Trust in Domains. In *IEEE Symposium on Security and Privacy* (2016).

[34] LIU, S., FOSTER, I., SAVAGE, S., VOELKER, G. M., AND SAUL, L. K. Who is .com? Learning to Parse WHOIS Records. In *ACM Internet Measurement Conference* (2015).

[35] MARICONTI, E., ONAOLAPO, J., AHMAD, S. S., NIKIFOROU, N., EGELE, M., NIKIFORAKIS, N., AND STRINGHINI, G. Why Allowing Profile Name Reuse Is A Bad Idea. In *European Workshop on System Security* (2016).

[36] MARICONTI, E., ONAOLAPO, J., AHMAD, S. S., NIKIFOROU, N., EGELE, M., NIKIFORAKIS, N., AND STRINGHINI, G. What's in a Name? Understanding Profile Name Reuse on Twitter. In *World Wide Web Conference* (2017).

[37] MOORE, T., AND EDELMAN, B. Measuring the Perpetrators and Funders of Typosquatting. In *Financial Cryptography and Data Security* (2010).

[38] MURPHY, K. DropCatch spends millions to buy FIVE HUNDRED more registrars. http://domainincite.com/21309-dropcatch-spends-millions-to-buy-five-hundred-more-registrars, 2016.

[39] MURPHY, K. Pheenix adds 300 more registrars to drop-catch arsenal. http://domainincite.com/21365-pheenix-adds-300-more-registrars-to-drop-catch-arsenal, 2016.

[40] NAMEJET. Downloads. http://www.namejet.com/Pages/Downloads.aspx.

[41] NAMEPROS. DesktopCatcher software. https://www.namepros.com/threads/desktopcatcher-software.873819/, 2015.

[42] NIKIFORAKIS, N., INVERNIZZI, L., KAPRAVELOS, A., VAN ACKER, S., JOOSEN, W., KRUEGEL, C., PIESSENS, F., AND VIGNA, G. You Are What You Include: Large-scale Evaluation of Remote JavaScript Inclusions. In *ACM Conference on Computer and Communications Security* (2012).

[43] POOL. Pending Delete List. http://www.pool.com/viewlist.aspx.

[44] SCHLAMP, J., GUSTAFSSON, J., WÄHLISCH, M., SCHMIDT, T. C., AND CARLE, G. The Abandoned Side of the Internet: Hijacking Internet Resources When Domain Names Expire. In *International Workshop on Traffic Monitoring and Analysis* (2015).

[45] SNAPNAMES. Auction Lists. https://snapnames.com/download.jsp.

[46] SNAPNAMES. Top Registrar Domains. https://snapnames.com/download.jsp.

[47] SZURDI, J., KOCSO, B., CSEH, G., SPRING, J., FELEGYHÁZI, M., AND KANICH, C. The Long "Taile" of Typosquatting Domain Names. In *USENIX Security Symposium* (2014).

[48] VISSERS, T., JOOSEN, W., AND NIKIFORAKIS, N. Parking Sensors: Analyzing and Detecting Parked Domains. In *Network and Distributed System Security Symposium* (2015).

[49] WANG, D. Y., SAVAGE, S., AND VOELKER, G. M. Juice: A Longitudinal Study of an SEO Botnet. In *Network and Distributed System Security Symposium* (2013).

[50] WEAVER, N., KREIBICH, C., AND PAXSON, V. Redirecting DNS for Ads and Profit. In *USENIX Workshop on Free and Open Communications on the Internet* (2011).