Operational validation of the registrant information

Maciej Korczyński
Grenoble Alpes University / KOR Labs

GAC Plenary Session on Registration Data Issues
October 18, 2026



Context

- INFERMAL: Inferential analysis of maliciously registered domains
- Investigate domain abuse from the attacker's perspective
- Identify factors driving malicious domain registrations
- Scope: Maliciously registered phishing domains
- Features: 73 features encompassing three latent factors:
  1. Registration attributes
  2. Proactive verification
  3. Reactive security practices
- GLM regression analysis: relationship between features and the concentration of phishing domains at the registrar-TLD level

Results

- Operational validation of the registrant information
- We test whether registrars verify contact email addresses and phone numbers during account creation or before domain purchase
- “When the validation of registrant information such as their phone number of email takes place during the account creation or before the domain purchase, it has a significant negative coefficient of -1.21 ($p < 0.001$) indicating that it is associated with a 70% decrease in malicious registrations”

Discussion

- Results should be interpreted with caution and may or may not be generalized into actions by registrars or TLDs.
- It is essential to consider the economic implications, the impact on legitimate users, and the likely response of attackers to adjustments, and the result of partial/full implementation.
- The more data-driven analysis we have, the better.

Questions



Motivation

- Cybercriminals exploit domains for: phishing, malware, spam, botnets
- Constantly register new domains to fuel attacks
- Prior studies show **high abuse** in specific registrars and TLDs
- No comprehensive research on **factors influencing** malicious registrations



Goal

- Investigate domain abuse from the **attacker's perspective**
- Identify factors driving malicious domain registrations

Approach – overview

- Scope: Maliciously registered phishing domains
- Features: 73 features encompassing three latent factors:
  1. Registration attributes
  2. Proactive verification
  3. Reactive security practices
- GLM regression analysis:
  1. Relationship between features and the concentration of phishing domains at the registrar-TLD level
  2. Features are favored by attackers alone or also by legitimate users

Datasets

- Phishing: APWG, PhishTank, OpenPhish
- Benign domain names: ICANN CZDS, Google CT logs, etc.
- Features:
  1. TLD-List (e.g., domain registration costs, discounts, free features) *
  2. Manually collected data (e.g., free API, API create user account, API register domain, restrictions)
  3. Active measurements (uptimes)

- Active WHOIS and DNS measurements

* https://tld-list.com/

Maliciously registered phishing and benign domains

- 534 K bloclisted URLs (Aug 2023 – Jan 2024)
- **108 K** domain names

- Excluding domains of benign services
- Active measurements (DNS, WHOIS) over one month to verify if the takedown occurred
- **28 K** registered maliciously

- Mapping between domains and daily-collected registration features
- **14 K** maliciously registered (165 TLDs, 31 registrars)

- Benign dataset of 15.4 K domains under 259 TLDs originating from 38 registrars

Rank	Registrar	TLD	#Domains
1.	NameSilo	`top`	1,807
2.	NameSilo	`com`	852
3.	GoDaddy	`com`	832
4.	Hostinger	`online`	764
5.	NameSilo	`info`	513
6.	Hostinger	`com`	479
7.	Namecheap	`com`	479
8.	Alibaba Cloud	`com`	327
9.	NameSilo	`xyz`	233
10.	Hostinger	`cloud`	225
11.	NameSilo	`buzz`	222
12.	Sav	`com`	211
13.	Alibaba Cloud	`shop`	197
14.	NameSilo	`us`	191
15.	Hostinger	`site`	179
16.	NameSilo	`life`	178
17.	NameSilo	`sbs`	171
18.	Hostinger	`shop`	156
19.	NameSilo	`cc`	149
20.	Alibaba Cloud	`top`	148

20 most frequently observed registrar/TLD pairs in our dataset of maliciously registered domain names

Selected features

1. Registration attributes

   - **Free API**: the registrar APIs enable users to search, purchase, and manage domains
   - **Free bulk search**: the capability to search multiple domains
   - **Available payment methods**: 24 boolean features for each payment method, including PayPal, Bitcoin, etc.
   - **Retail pricing:** domain name registration prices
   - **Discounts:** deducting a fixed amount or % from the regular price
   - **Pricing terms:** might apply only to a limited number of domains or new customers
   - **Free web hosting, free DNS, free email account:** included for free in each domain registration



Selected features

2. Proactive verification

- **Operational validation of the registrant contact details**: Test whether contact details (email/phone) are verified during account creation or before domain purchase.

- **Domain registration warnings and restrictions**: three labels defined:
    i. `9e86e6d5d4c676441da` (the first 20 characters of the MD5hash of "DNS abuse"),
    ii. `office365-my-account`
    iii. `facebook-login-page`

  For each registrar-TLD pair, we proceed to the payment prompt.

- **Registration restrictions**: 14 boolean features, e.g., local presence required, ID required, professionals only

Selected features

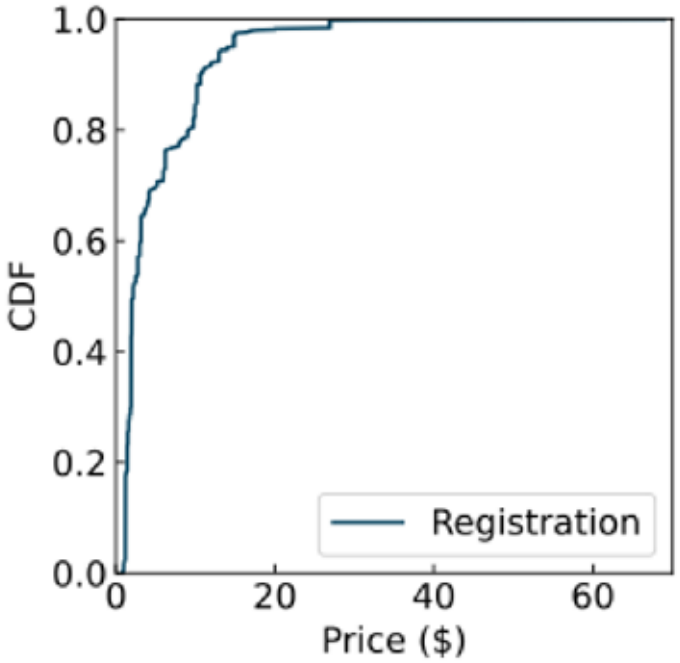
3. Reactive security practices: malicious domain name uptimes (with and without notifications)

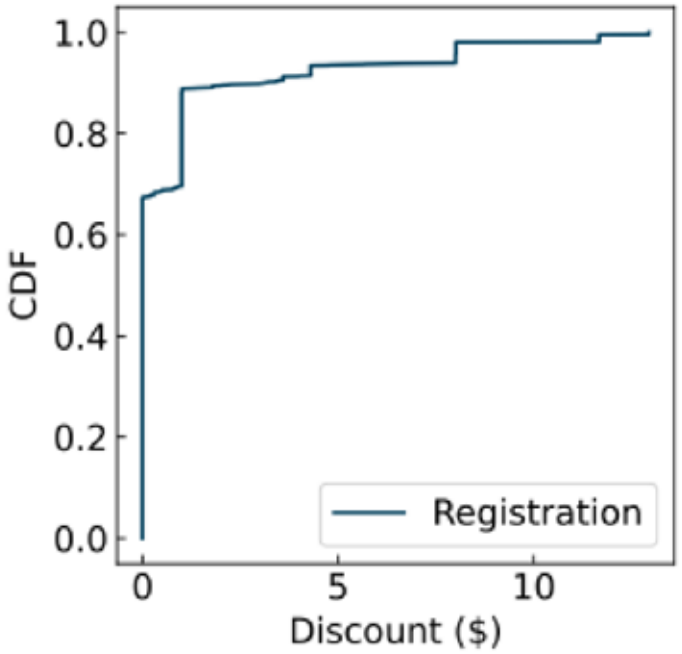
   - WHOIS/DNS measurements
   - 5 minutes, 15 m, 30 m, 1 hour, 2 h, 3 h, 4 h, 5 h, 6 h, 12 h, 24 h, 36 h, and 48 h after blocklisting, and then every 12 hours
   - for a subset of maliciously registered domain names, notifications are sent to registrars

Descriptive Analysis of Features

Prices and discounts: Registration

- Prices range from $0.78 to $69, with nearly 50% costing $2 or less

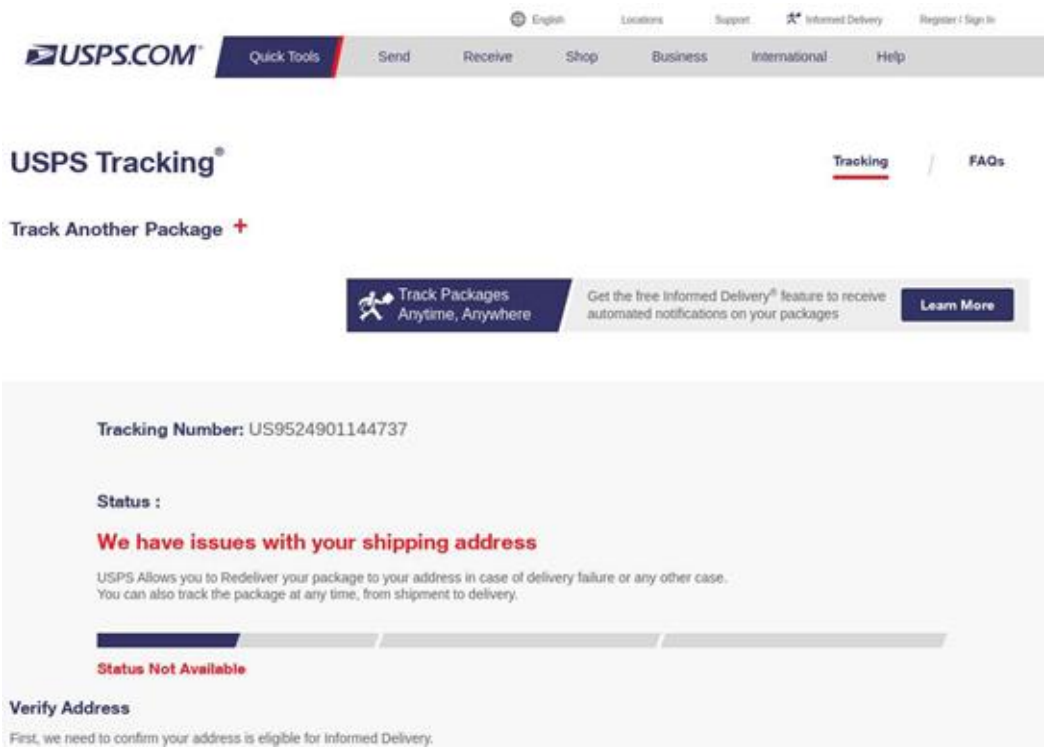




Descriptive Analysis of Features

Prices and discounts: Registration

- Examples of expensive domains include usps.bar ($69), support-fb.sh ($59.99), and dhlcenter.net ($56)



Descriptive Analysis of Features

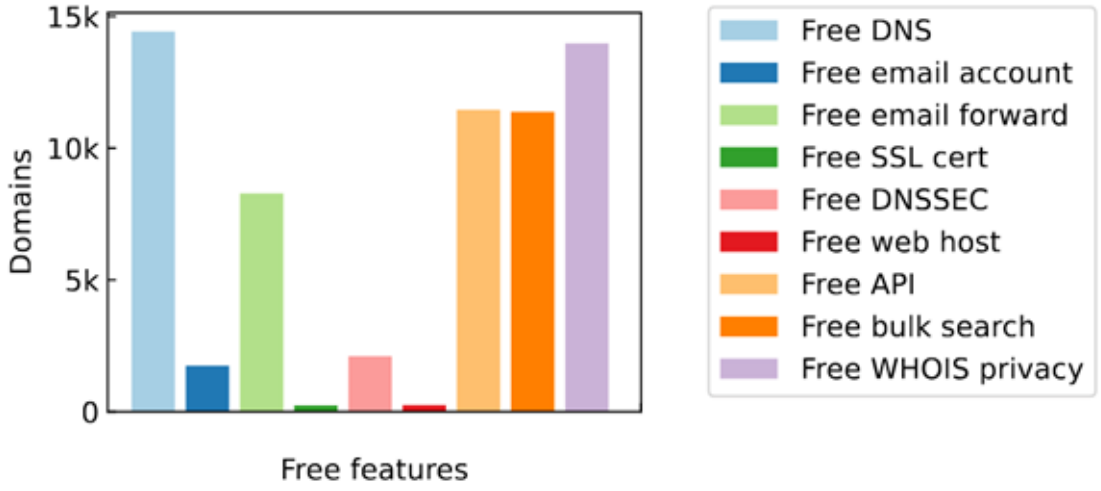
Registration prices and discounts:

- Registration prices may be subject to various terms (e.g., 4,423, reduced registration prices were valid for one domain), discounts to new customers only

Descriptive Analysis of Features

Free features

- A free API is offered by 16 of the 31 registrars we examined
- Four registrars permit the automated account creation (e.g., as a subaccount under an existing API user)
- 18 registrars offer a "bulk search" to check availability and prices for 20 to 10 k+



Descriptive Analysis of Features

Payment methods

- 13 are supported by the 31 analyzed registrars. Bitcoin supported in more than two-thirds of cases.

Domain Name Registrant Data

- Phone verification is rare: 23 registrars check syntax, and only 6 validate operationally

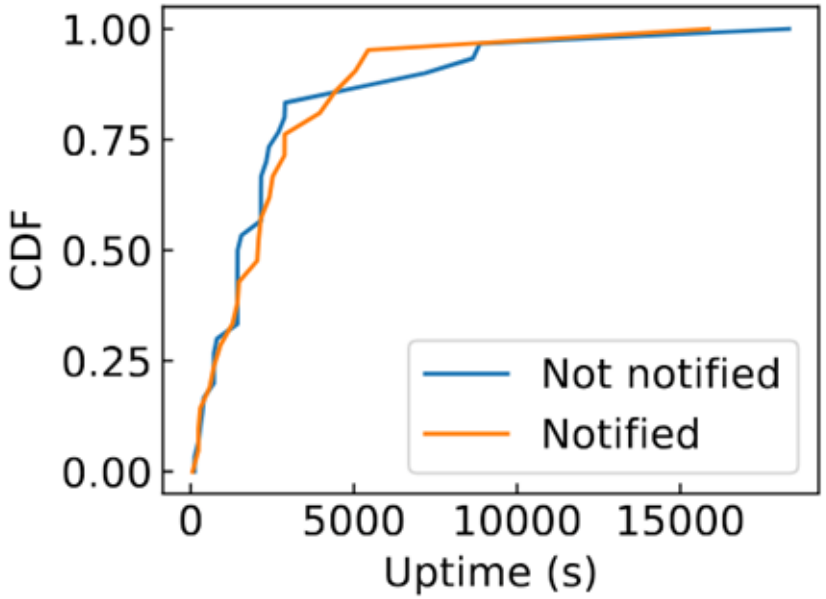
Prevention of Trademark Infringement

- Two registrars blocked trademarked domains from being added to the cart

Descriptive Analysis of Features

Malicious Domain Uptimes

- Similar results at the domain and registrar levels



CDF of uptimes for notified and not notified registrars

Driving Factors of Domain Abuse

Model 1: Relationship between features and the concentration of phishing domains at the **registrar-TLD** level

Driver	Type	Correlation with abuse counts	Increase
Retail registration price	Numerical	Weak positive	1$↓ (6.6%↑)
Retail registration discounts	Numerical	Positive	1$↓ (49%↑)
Cryptocurrency payment(s) available	Boolean	Positive	30%
APIs to register domains or to create accounts available	Boolean	Strong positive	401%

Driving Factors of Domain Abuse

Our analysis suggests that while initial pricing plays a role, attractiveness to attackers likely results from a combination of factors

Driver	Correlation with abuse counts	Correlation with abuse counts	Increase
Free DNS service	Boolean	Positive	205%
Free hosting service	Boolean	Positive	88%
Presence of restrictions (e.g., commitment required, local presence, professionals only)	Boolean	Negative	63%
Validation of email/phone present	Boolean	Negative	70%
Shorter uptimes	Numerical	Statistically significant but negligible correlation	~0%

Discussion and conclusions

- Key factors driving malicious domain registrations from the **attacker's perspective**.
- This study did not include instances of benign domains that have been compromised, for example, at the website or hosting level.
- Results should be interpreted with caution and may or may not be generalized into actions by registrars or TLDs.
- Some factors are combined and involve a variety of features.
- Attractiveness to attackers likely results from a combination of factors.
- It is essential to consider the economic implications, the impact on legitimate users, and the likely response of attackers to adjustments, the result of partial/full implementation.



Exposing the Roots of DNS Abuse: A Data-Driven Analysis of Key Factors Behind Phishing Domain Registrations

Yevheniya Nosyk, Maciej Korczyński, Carlos Gañán, Sourena Maroofi, Jan Bayer, Zul Odgerel, Samaneh Tajalizadehkhoob, Andrzej Duda
KOR Labs / Grenoble Alpes University
ICANN org



ACM CCS'25



Acknowledgements

We would like to thank the ICANN OCTO-SSR research team (Carlos and Samaneh) for scientific discussions, ICANN for funding this research, the Anti-Phishing Working Group, Phishtank, and OpenPhish for access to their feeds, and Spamhaus and SURBL, whose datasets helped us filter out malicious domains from the benign list we sampled. We thank Rowena Schoo, Graeme Bunton (Netbeacon Institute), Siôn Lloyd (ICANN) for their insightful comments on the presentation.









Contact information

Yevheniya Nosyk, Maciej Korczyński, Sourena Maroofi, Jan Bayer, Zul Odgerel, Andrzej Duda (KOR Labs / Grenoble Alpes Univ.)

Project website: https://infermal.korlabs.io/

KOR Labs
contact@korlabs.io

ICANN OCTO
samaneh.tajali@icann.org

Questions

