

Insights and Clarifications on the INFERMAL Study

OCTO-SSR
10 June 2025



TABLE OF CONTENTS

EXECUTIVE SUMMARY	3
PROJECT OBJECTIVES AND METHODOLOGY	3
KEY FINDINGS	4
STUDY LIMITATIONS	5
CONSIDERATIONS FOR INTERPRETATION	5
LOOKING AHEAD	6
CONCLUSION	6

EXECUTIVE SUMMARY

The Inferential Analysis of Maliciously Registered Domains ([INFERMAL](#)) is a two-year research project led by the Security, Stability, and Resiliency (SSR) Research team within ICANN's Office of the Chief Technology Officer (OCTO) and conducted by KOR Labs. Funded by ICANN, the study provides a statistically rigorous analysis of malicious domain registrations, with a focus on understanding attacker preferences at the time of domain name registration.

INFERMAL addresses a long-standing question in the Internet governance and DNS security communities: Why do malicious domain registrations tend to cluster at certain registrars and top-level domains (TLDs)? By analyzing more than 29,000 domains – half malicious, half benign – across 73 service features, the study identifies which registrar and registry attributes are most associated with phishing abuse.

Key findings highlight that cost, automation, and lack of identity verification significantly increase the likelihood of abuse. In contrast, proactive controls, such as Know Your Business Customer (KYBC) requirements and restricted API access, correlate with lower abuse rates. Reactive measures, such as domain takedown speed, were found to have limited deterrent effect.

The [final report](#) offers data-driven guidance for the ICANN community and contracted parties seeking to design effective DNS Abuse mitigation strategies. It also contributes to broader discussions on risk-based policy approaches, balancing deterrence with operational flexibility for legitimate registrants.

The final results were [presented at ICANN81](#) in Istanbul and during a February 2025 webinar. The research has been peer-reviewed and accepted for publication by a leading computer security conference.

PROJECT OBJECTIVES AND METHODOLOGY

The central question posed by the INFERMAL project was: What registrar and registry-level features are preferred (or avoided) by malicious actors registering domains for phishing? The study examined over 29,000 domains, consisting of 14,500 classified as malicious and 15,400 as benign.

For each domain, researchers collected a set of 73 features related to registrar services and policies. These were categorized into three groups:

1. **Registration Attributes** – Pricing, API access, payment methods, bundled services
2. **Proactive Verification** – Identity checks, delays in activation, Know Your Business Customer (KYBC) procedures
3. **Reactive Security Practices** – Measures taken after abuse, such as domain suspension speed

Using Generalized Linear Models (GLMs), a well-established statistical modeling technique, researchers analyzed the relationship between these features and the likelihood of a domain being malicious.

KEY FINDINGS

Economic Incentives Influence Attacker Preferences

The most consistent finding was that malicious actors are highly price-sensitive. On average, domains used for phishing were registered at a significantly lower cost – USD 4.71 – compared to benign domains, which averaged USD 8.62. Discounted pricing and bulk registration opportunities were strongly associated with abuse.

Even when discounts were limited to first-time users, attackers exploited unrestricted application programming interfaces (APIs) to create multiple accounts and access low-cost registrations at scale. This underscores how economic incentives, particularly when paired with automation, can increase vulnerability to abuse.

Free Services and APIs Increase Risk

Registrars that offered free DNS services and bundled web hosting were associated with higher rates of malicious registrations. These services lower the cost and complexity for attackers, though the analysis acknowledges that they are also used by legitimate registrants.

More notable was the role of registrar APIs. API access was linked to a 401 percent increase in malicious domain registrations relative to the model's baseline. APIs enable bulk, automated registration and configuration, a capability heavily exploited by attackers to operate phishing infrastructure efficiently.

To mitigate this, the report suggests that API access should be restricted to known, vetted users. This policy has already been adopted by some registrars and could reduce abuse without significantly impacting legitimate operations.

Proactive Measures Reduce Abuse

The study identified proactive restrictions at the point of registration as highly effective in deterring abuse. Registrars employing identity verification, registration delays, or KYBC practices saw a 63 percent decrease in abuse rates. These measures did not appear to deter legitimate registrants, suggesting a favorable cost-benefit tradeoff.

The European Union's eIDAS Regulation, which provides a standardized framework for digital identity verification, was discussed as a potential model for implementing KYBC at scale. However, the report cautions that attackers may adapt through tactics such as digital identity theft or use of stolen credentials.

The study contrasted two examples to illustrate this complexity:

- The .dk TLD, which mandates KYBC and reports low abuse levels
- The .cn TLD, which also requires identity verification but remains among the most abused

This comparison highlights the importance of policy implementation quality and broader systemic context.

Reactive Measures Are Less Effective

INFERMAL also evaluated the impact of reactive measures, such as domain takedown speed following blocklisting. The analysis showed that time-to-suspension had only a marginal effect on abuse concentration and little influence on attacker behavior.

Given that phishing campaigns often yield results within hours, attackers may not require long operational windows. Thus, proactive deterrence—through economic, procedural, and technical controls—remains a more effective strategy than reactive enforcement.

STUDY LIMITATIONS

While the study's statistical modeling and dataset were robust, several limitations are acknowledged:

1. **Registrar-Level Feature Granularity:** The analysis reflects services offered by registrars broadly, not specific choices made during individual domain registrations. For example, a registrar may offer API access and accept cryptocurrency payments, but it is not always possible to confirm whether these features were used in a specific registration.
2. **Partial Coverage of TLDs:** Some TLDs lack accessible WHOIS data (e.g., .gr), are partially restricted (e.g., .es), or provide minimal details (e.g., .de). These gaps limit data completeness, although the majority of analyzed TLDs had sufficient transparency.
3. **Domain Classification Challenges:** The methodology prioritized excluding compromised domains and false positives. Nevertheless, sophisticated phishing campaigns using evasion tactics may still appear benign. Benign domain samples were filtered against known blocklists and subjected to additional quality checks.
4. **Model Interpretation:** Percentages like the 401 percent increase associated with API access must be interpreted within the full statistical context. GLMs account for interactions among all variables. These results do not imply a standalone causal relationship but rather an observed correlation while holding other factors constant.

Additionally, the report combined certain features into composite variables. Payment methods were grouped into cryptocurrency, banking, and digital wallets. Similarly, restrictions and verification processes were aggregated into broader prevention-related variables.

CONSIDERATIONS FOR INTERPRETATION

The findings of the INFERMAL study provide actionable insights but must be contextualized carefully:

- **No Single Variable Is Determinative:** The study does not suggest that one factor alone determines abuse. Rather, it is the confluence of features—low cost, automated registration, minimal verification—that increases risk.
- **Results Are Context-Dependent:** The effectiveness of measures such as KYBC depends on how they are implemented and the surrounding regulatory or operational environment.
- **Statistical Models Reflect General Trends:** The 401 percent API-related increase reflects a correlation, not a guarantee of abuse. Changes in other model inputs could alter this figure.
- **Evasion and Adaptation Are Real Risks:** Even effective interventions like identity verification could be circumvented through methods such as stolen ID documents, underscoring the importance of holistic, layered defense strategies.

LOOKING AHEAD

INFERMAL originated as a community-driven research proposal aligned with recommendations from the Competition, Consumer Trust, and Consumer Choice Review (CCT) and the second Security, Stability, and Resiliency Review (SSR2). The project has provided the most granular view to date of how attacker behavior aligns with registrar offerings and registration processes.

ICANN welcomes feedback from the community on potential follow-up work. Future research may explore:

- Abuse patterns beyond phishing, such as malware and spam
- Comparative studies across country-code TLDs
- Longitudinal studies of domain lifecycle and abuse evolution

Community input will help shape the direction of continued research on DNS Abuse and inform evidence-based policy decisions.

CONCLUSION

The INFERMAL project represents a significant step forward in understanding attacker behavior in domain registration. By shifting the lens from abuse outcomes to attacker incentives, the study offers a framework for proactive, risk-based interventions. It also highlights the role of registrar and TLD policy decisions in shaping the threat landscape. Well-targeted mitigation strategies, such as restricted API access, identity verification, and pricing transparency, can reduce abuse while preserving access for legitimate users.

To discuss the [INFERMAL report](#) or propose future studies, please contact the ICANN OCTO team at octo@icann.org.



One World, One Internet

Visit us at icann.org



[@icann](https://twitter.com/icann)



facebook.com/icannorg



youtube.com/icannnews



flickr.com/icann



linkedin.com/company/icann



soundcloud.com/icann



instagram.com/icannorg