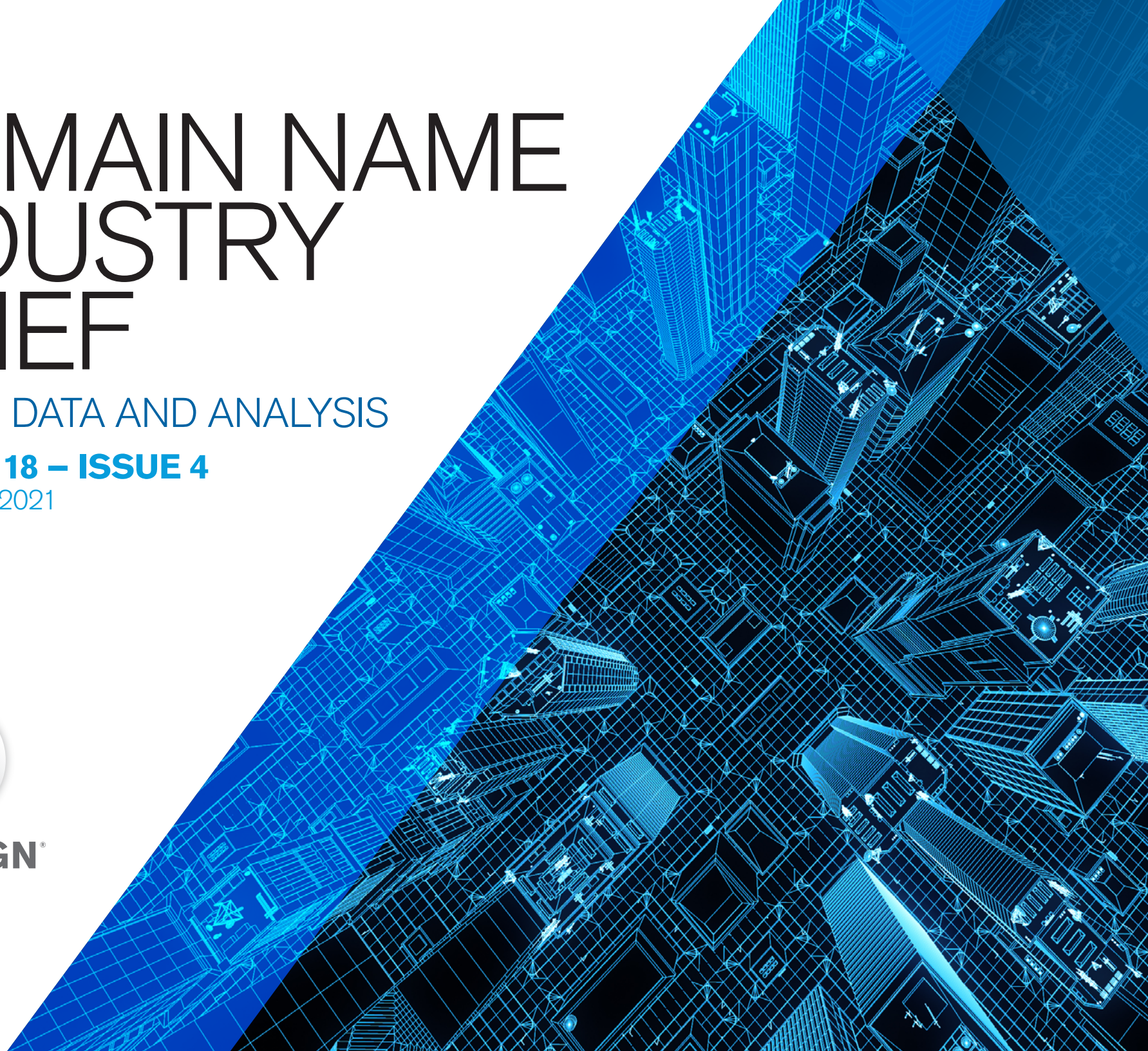
THE DOMAIN NAME INDUSTRY BRIEF

Q3 2021 DATA AND ANALYSIS

VOLUME 18 – ISSUE 4
DECEMBER 2021



VERISIGN®

THE DOMAIN NAME INDUSTRY BRIEF

As a global provider of domain name registry services and internet infrastructure, Verisign reviews the state of the domain name industry each quarter through a variety of statistical and analytical research, as well as relevant industry insight. Verisign provides this brief to highlight important trends in domain name registrations, including key performance indicators and growth opportunities, to industry analysts, media and businesses.

EXECUTIVE SUMMARY

The third quarter of 2021 closed with 364.6 million domain name registrations across all top-level domains, a decrease of 2.7 million domain name registrations, or 0.7%, compared to the second quarter of 2021.[1,2] Domain name registrations have decreased by 6.1 million, or 1.6%, year over year.[1,2]

The .com and .net TLDs had a combined total of 172.1 million domain name registrations in the domain name base[3] at the end of the third quarter of 2021, an increase of 1.5 million domain name registrations, or 0.9%, compared to the second quarter of 2021. The .com and .net TLDs had a combined increase of 8.3 million domain name registrations, or 5.1%, year over year. As of Sept. 30, 2021, the .com domain name base totaled 158.6 million domain name registrations, and the .net domain name base totaled 13.5 million domain name registrations.

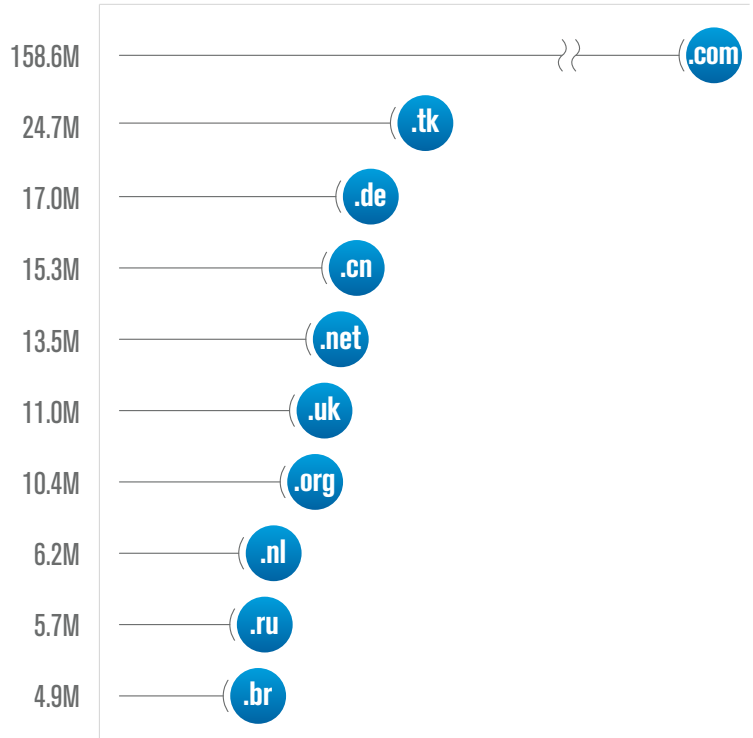
New .com and .net domain name registrations totaled 10.7 million at the end of the third quarter of 2021, compared to 10.9 million domain name registrations at the end of the third quarter of 2020.

Total country-code TLD domain name registrations were 152.9 million at the end of the third quarter of 2021, a decrease of 4.8 million domain name registrations, or 3.0%, compared to the second quarter of 2021.[1,2] ccTLDs decreased by 7.7 million domain name registrations, or 4.8%, year over year.[1,2]

Total new gTLD domain name registrations were 23.5 million at the end of the third quarter of 2021, an increase of 0.6 million domain name registrations, or 2.7%, compared to the second quarter of 2021. ngTLDs decreased by 6.7 million domain name registrations, or 22.2%, year over year.

TOP 10 LARGEST TLDs BY NUMBER OF REPORTED DOMAIN NAMES

Source: ZookNIC, Q3 2021; Verisign, Q3 2021; Centralized Zone Data Service, Q3 2021



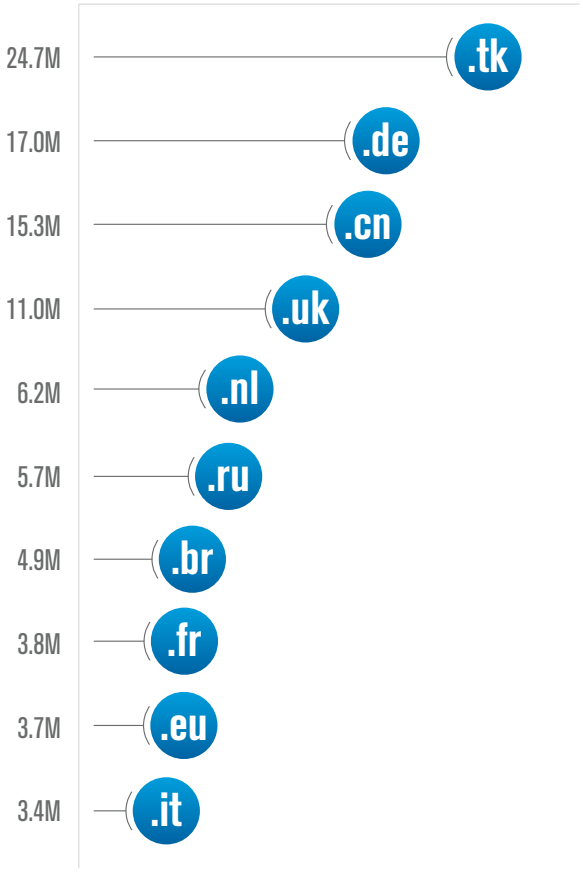
As of Sept. 30, 2021, the largest TLDs by number of reported domain names were .com, .tk, .de, .cn, .net, .uk, .org, .nl, .ru and .br.[1,2,4]

TOP 10 LARGEST ccTLDs BY NUMBER OF REPORTED DOMAIN NAMES

Source: ZookNIC, Q3 2021
For further information on *The Domain Name Industry Brief* methodology, please refer to the last page of this brief.

Total ccTLD domain name registrations were 152.9 million at the end of the third quarter of 2021, a decrease of 4.8 million domain name registrations, or 3.0%, compared to the second quarter of 2021.[1,2] ccTLDs decreased by 7.7 million domain name registrations, or 4.8%, year over year.[1,2] Excluding .tk, ccTLD domain name registrations decreased by 4.8 million in the third quarter of 2021, or 3.6%, compared to the second quarter of 2021. ccTLDs, excluding .tk, decreased by 4.9 million domain name registrations, or 3.7%, year over year.

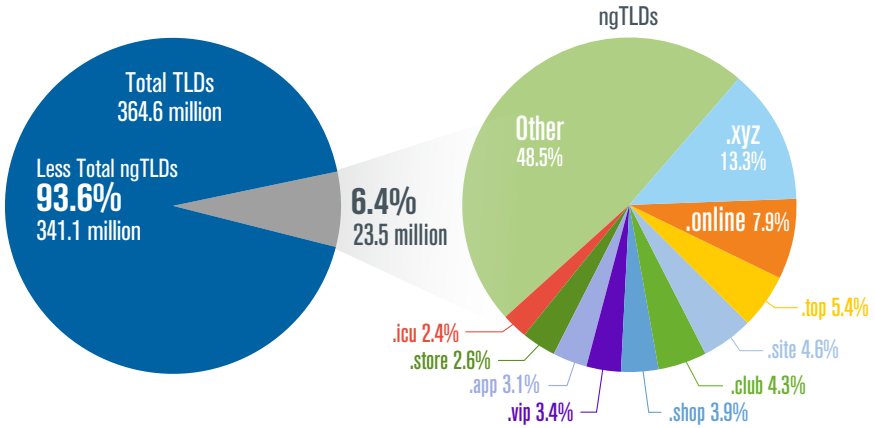
The top 10 ccTLDs, as of Sept. 30, 2021, were .tk, .de, .cn, .uk, .nl, .ru, .br, .fr, .eu and .it.[1,2] As of Sept. 30, 2021, there were 308 global ccTLD extensions delegated in the root zone, including IDNs, with the top 10 ccTLDs comprising 62.7% of all ccTLD domain name registrations.[1,2]



ngTLDs AS PERCENTAGE OF TOTAL TLDs

Source: ZookNIC, Q3 2021; Verisign, Q3 2021; and Centralized Zone Data Service, Q3 2021

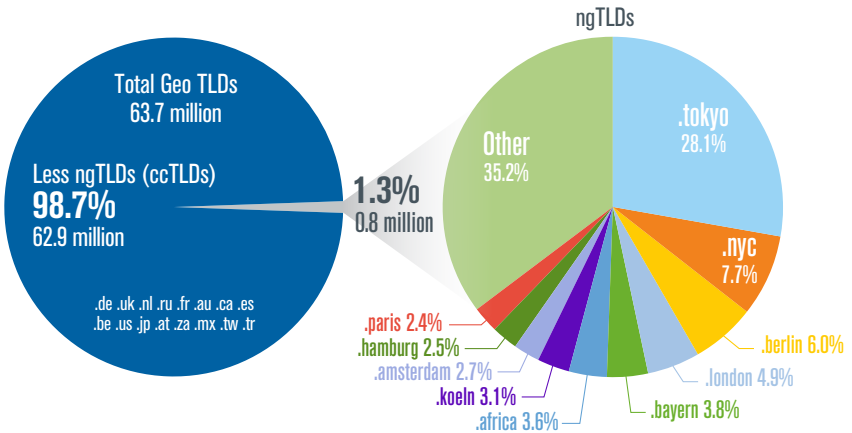
The top 10 ngTLDs represented 51.5% of all ngTLD domain name registrations. The following chart shows ngTLD domain name registrations as a percentage of overall TLD domain name registrations, of which they represent 6.4%. In addition, the chart on the right highlights the top 10 ngTLDs as a percentage of all ngTLD domain name registrations for the third quarter of 2021.



GEOGRAPHICAL ngTLDs AS PERCENTAGE OF TOTAL CORRESPONDING GEOGRAPHICAL TLDs

Source: ZookNIC, Q3 2021 and Centralized Zone Data Service, Q3 2021

As of Sept. 30, 2021, there were 47 ngTLDs delegated that met the following criteria: 1) had a geographical focus and 2) had more than 1,000 domain name registrations since entering general availability. The chart on the left summarizes the domain name registrations as of Sept. 30, 2021, for the listed ccTLDs and the corresponding geographical ngTLDs within the same geographic region. In addition, the chart on the right highlights the top 10 geographical ngTLDs as a percentage of the total geographical TLDs.



NEW ON THE VERISIGN BLOG / July – September 2021

INDUSTRY INSIGHTS: RDAP BECOMES INTERNET STANDARD

A look back at the registry data model, given the evolution from WHOIS to the RDAP protocol, and an examination of how the RDAP protocol can help improve upon the more traditional, WHOIS-based registry models.

AFILIAS' RULE VIOLATIONS CONTINUE TO DELAY .WEB

The final decision issued on May 20 in the Independent Review Process brought by Afilias against the Internet Corporation for Assigned Names and Numbers rejected Afilias' petition to nullify the results of the public auction for .web, and it further rejected Afilias' demand to have it be awarded .web.

WEBSITES, BRANDED EMAIL REMAIN KEY TO SMB INTERNET SERVICES

The findings of our independent survey of online consumers suggest that websites and branded email continue to be critical components of many businesses' online presence, essential to supporting consumer confidence and enabling effective interaction with customers.

THE TEST OF TIME AT INTERNET SCALE: VERISIGN'S DANNY MCPHERSON RECOGNIZED WITH ACM SIGCOMM AWARD

The ACM SIGCOMM 2021 conference series recognized the enduring value of the Internet Inter-Domain Traffic research paper with the prestigious Test of Time Paper Award, given to "an outstanding paper whose contents are still a vibrant and useful contribution today."

ARTICLE

INDUSTRY INSIGHTS: ONGOING COMMUNITY WORK TO MITIGATE DOMAIN NAME SYSTEM SECURITY THREATS

This article is an abridged version of a blog originally published on December 6, 2021.

Author: Keith Drazek, Vice President - Public Policy & Government Relations

For over a decade, the Internet Corporation for Assigned Names and Numbers (ICANN) multi-stakeholder community has engaged in an extended dialogue on the topic of DNS abuse, and the need to define, measure and mitigate DNS-related security threats. Within their respective roles and capabilities, the members of this community have important parts to play in identifying, reporting and mitigating illegal or harmful behavior.

It's important to understand ICANN's central role in preserving the security, stability, resiliency and global interoperability of the internet's unique identifier system, and also the limitations established within ICANN's bylaws. For example, per its bylaws, ICANN "shall not regulate" services that use the DNS, or the content that those services carry or provide. As such, ICANN's role is important, but limited.

ICANN's gTLD contracted parties, both registries and registrars, continue to engage with ICANN, and other stakeholders and community interest groups, to address key factors related to effective and appropriate DNS security threat mitigations across the DNS ecosystem, including:

- Determining the roles and responsibilities of the various service providers
- Delineating categories of threats
- Understanding the precise operational and technical capabilities of various types of providers
- Defining the role of third-party "trusted notifiers" and the processes that materialize as a result
- Promoting administrative and operational scalability in trusted notifier engagements
- Determining the necessary safeguards around liability, due process and transparency
- Supporting ICANN's role in coordination and facilitation

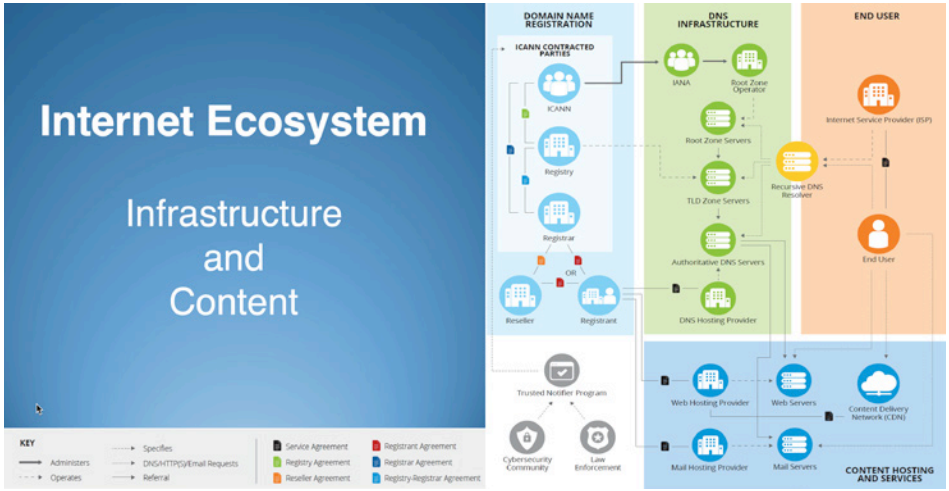
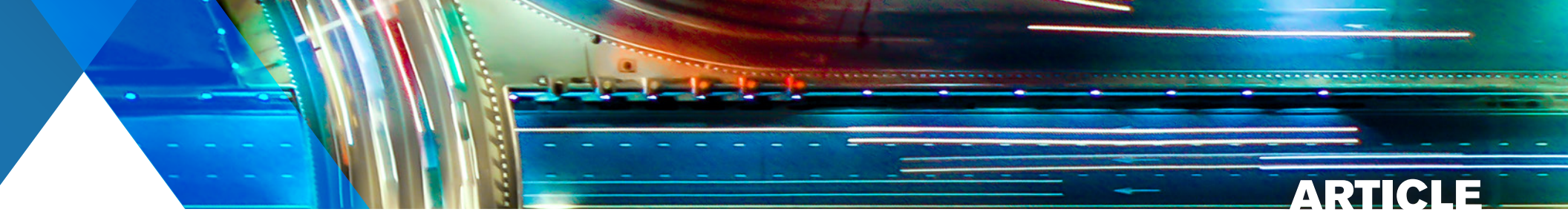


Fig 1: The Internet Ecosystem

Definitions of Online Abuse

To better understand the various roles, responsibilities and processes, it's important to first define illegal and abusive online activity. While perspectives may vary, the emerging consensus on definitions and terminology is that these activities can be classified into four categories:

- **DNS security threats**: defined as being "composed of five broad categories of harmful activity [where] they intersect with the DNS: malware, botnets, phishing, pharming, and spam when it serves as a delivery mechanism for the other forms of DNS Abuse."



- **Infrastructure abuse**: a broader set of security threats that can impact the DNS itself, such as denial-of-service, or /distributed denial-of-service attacks, DNS cache poisoning, protocol-level attacks and exploitation of implementation vulnerabilities.
- **Illegal content**: material that is illegal and is hosted on websites that are accessed via domain names in the DNS hierarchy, including the illegal sale of controlled substances and/or regulated goods, the distribution of child sexual abuse material (CSAM), and proven intellectual property infringement.
- **Abusive content**: information hosted on websites using the domain name infrastructure that is deemed "harmful," either under applicable law or norms, which could include scams, fraud, misinformation or intellectual property infringement, where illegality has yet to be established by a court of competent jurisdiction.

ICANN Efforts & Community Inputs on DNS Abuse

The ICANN organization has been actively involved in advancing work on DNS abuse, including the Domain Abuse Activity Reporting (DAAR) system for studying and reporting threats across top-level domain registries, as well as developing a framework to help registry operators improve their own DNS security posture, and serving as a catalyst for increased community attention and action on DNS abuse.

ICANN continues to develop new initiatives in this arena, including: (1) expanding DAAR to integrate some ccTLDs, and to eventually include registrar-level reporting; (2) work on abusive COVID-related domain names; (3) contributions to the development of a Domain Generating Algorithms (DGA) framework and facilitating waivers to allow registries to act on botnets at scale; and (4) plans to establish a DNS abuse ICANN Board caucus.

These ICANN community group inputs have helped bring additional clarity to the topic of DNS abuse, and have encouraged ICANN, registries, and registrars to look for improved mechanisms to address abuse. Collectively, registries and registrars have engaged with nearly all groups in the ICANN community, and have produced important documents related to DNS abuse definitions, registry actions, registrar abuse reporting, domain generating algorithms, and trusted notifiers. These all represent significant progress in contextualizing the roles, responsibilities and capabilities of registries and registrars, and Verisign has been an important contributor to these initiatives.

Other Groups and Actors focused on DNS Security

Groups outside of ICANN's immediate multi-stakeholder community have also made important contributions to DNS abuse mitigation efforts:

Internet & Jurisdiction Policy Network

The I&JPN addresses tension between the cross-border internet and national jurisdictions, facilitating a global engagement for over 400 key entities from governments, the world's largest internet companies, technical operators, civil society groups, academia and international organizations from over 70 countries. Verisign has supported the I&JP since its inception, and its work has been instrumental in developing multi-stakeholder inputs on issues such as trusted notifier.

DNS Abuse Institute

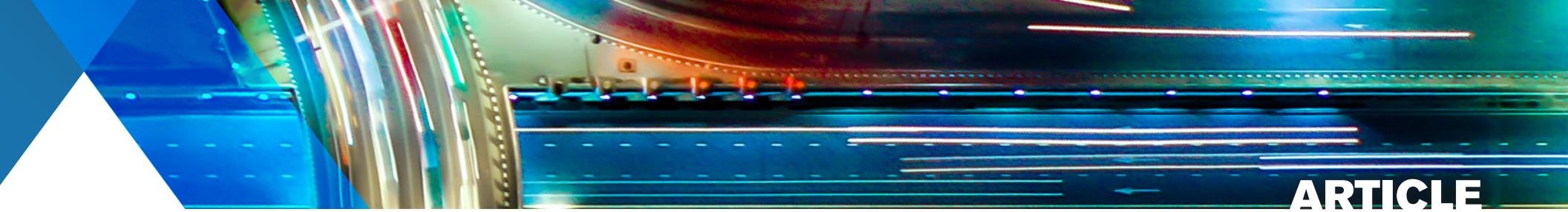
The DNS Abuse Institute develops outcome-based initiatives to create recommended practices, foster collaboration and develop industry-shared solutions to combat the five broad categories of DNS security threats.

Global Cyber Alliance

The Global Cyber Alliance is a nonprofit organization dedicated to making the internet a safer place by reducing cyber risk. The GCA builds programs, tools, and partnerships to sustain a trustworthy internet to enable social and economic progress for all.

ECO "topDNS" DNS Abuse Initiative

Eco is the largest association of the internet industry in Europe and a long-standing advocate of responsibility and self-regulation. The eco "topDNS" initiative will help bring together stakeholders with an interest in combating and mitigating DNS security threats, and Verisign is a supporter of this new effort.



Other Community Groups

Verisign contributes to the anti-abuse, technical and policy communities, continuously engaging with ICANN and an array of other industry partners to help ensure the continued safe and secure operation of the DNS, such as the Anti-Phishing and Messaging, Malware and Mobile Anti-Abuse Working Groups, FIRST and the Internet Engineering Task Force.

What Verisign is Doing Today

As a DNS ecosystem industry leader, Verisign supports cross-community efforts and engages directly by:

- **Monitoring for abuse**: Combating abuse starts with detecting abusive behavior in our systems and addressing it, working closely with a range of actors, including trusted notifiers, to ensure our abuse mitigation actions are informed by subject matter expertise and procedural rigor.
- **Blocking and redirecting abusive domain names**: Blocking and redirecting certain domain names identified as security threats, including botnets, helps protect the DNS infrastructure and minimize potential threats. Earlier this year, we took action against a botnet family responsible for a disproportionate amount of total global DNS queries.
- **Avoiding 'disposable' domain registrations**: Heavily discounted pricing strategies may promote short-term sales, but also attract registrants who might be engaged in abuse. Some security threats exploit the ability to register multiple 'disposable' domain names rapidly and cheaply.
- **Partnering with law enforcement and government**: We have maintained constructive relationships with U.S. and international law enforcement and government agencies to help address threats to operational applications and critical internet infrastructure, as well as illegal activity associated with domain names.
- **Adhering to contractual obligations**: Our contractual frameworks, policies and agreements help provide an effective legal framework to discourage abusive domain name registrations and promote good hygiene within the registrar channel.
- **Entering into a binding Letter of Intent ("LOI")** with ICANN that commits both parties to cooperate in taking a leadership role in combatting security threats, including the development of best practices, educating the broader ICANN community, and supporting activities that preserve and enhance the security, stability and resiliency of the DNS. Verisign also made a substantial financial commitment in direct support of these important efforts.

Trusted Notifiers

Third-party trusted notifiers work to identify illegal and abusive activities, and report to the appropriate actor in the DNS ecosystem. Verisign's recent coordination with the U.S. National Telecommunications and Information Administration and Food and Drug Administration in combating illegal online opioid sales has been insightful as a possible approach for third-party trusted notifier engagement. In addition, we engage directly with the Internet Watch Foundation and law enforcement in combating CSAM online. Discussions around trusted notifiers and an appropriate framework for engagement are ongoing, with active participation and commitment from Verisign, to explore how such notifications can be formalized and supported at scale.

Conclusion

DNS abuse and DNS-related security threat mitigation are important topics in the ICANN community. The DNS ecosystem has been constructively engaged in efforts to reduce the level and impact of malicious activity in the DNS. The ICANN community's focus on DNS abuse has been helpful and significant progress has been made, but more work is needed. As we look ahead to 2022, Verisign remains committed to leading and collaborating as the community works toward these important goals.

VERISIGN®

ABOUT VERISIGN

Verisign, a global provider of domain name registry services and internet infrastructure, enables internet navigation for many of the world's most recognized domain names. Verisign enables the security, stability and resiliency of key internet infrastructure and services, including providing root zone maintainer services, operating two of the 13 global internet root servers and providing registration services and authoritative resolution for the .com and .net top-level domains, which support the majority of global e-commerce. To learn more about what it means to be Powered by Verisign, please visit verisign.com.

LEARN MORE

To view the average daily number of queries Verisign processes, please go to the "Explore our Capabilities" section at verisign.com. To access the archives for *The Domain Name Industry Brief*, please go to verisign.com/dnibarchives. Email your comments or questions to domainbrief@verisign.com.

METHODOLOGY

The data presented in this brief, including quarter-over-quarter and year-over-year metrics, reflects information available to Verisign at the time of this brief and may incorporate changes and adjustments to previously reported periods based on additional information received since the date of such prior reports, so as to more accurately reflect the growth rate of domain name registrations. In addition, the data available for this brief may not include data for all of the 308 ccTLD extensions that are delegated to the root zone, and includes only the data available at the time of the preparation of this brief.

For gTLD and ccTLD data cited with ZookNIC as a source, the ZookNIC analysis uses a comparison of domain name root zone file changes supplemented with other authoritative data sources. For more information, see zooknic.com.

1 The figure(s) includes domain names in the .tk ccTLD. .tk is a ccTLD that provides free domain names to individuals and businesses. Revenue is generated by monetizing expired domain names. Domain names no longer in use by the registrant or expired are taken back by the registry and the residual traffic is sold to advertising networks. As such, there are no deleted .tk domain names. The .tk zone reflected here is based on data from Q4 2020, which is the most recent data available. https://www.businesswire.com/news/home/20131216006048/en/Freenom-Closes-3M-Series-Funding#.UxeUGNJDv9s.

2 The generic TLD, ngTLD and ccTLD data cited in this brief: (i) includes ccTLD Internationalized Domain Names (IDNs), (ii) is an estimate as of the time this brief was developed and (iii) is subject to change as more complete data is received. Some numbers in this brief may reflect standard rounding.

3 The domain name base is the active zone plus the number of domain names that are registered but not configured for use in the respective TLD zone file plus the number of domain names that are in a client or server hold status. The .com and .net domain name registration figures are as reported in Verisign's most recent SEC filings.

4 Line break indicates that the .com line has been shortened for display considerations.