THE
DOMAIN NAME INDUSTRY BRIEF

VOLUME 18 – ISSUE 1
MARCH 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 fourth quarter of 2020 closed with 366.3 million domain name registrations across all top-level domains (TLDs), a decrease of 4.4 million domain name registrations, or 1.2 percent, compared to the third quarter of 2020.[1,2] Domain name registrations have grown by 4.0 million, or 1.1 percent, year over year.[1,2]

Total country-code TLD (ccTLD) domain name registrations were 158.9 million at the end of the fourth quarter of 2020, a decrease of 1.7 million domain name registrations, or 1.0 percent, compared to the third quarter of 2020.[1,2] ccTLDs increased by 1.3 million domain name registrations, or 0.8 percent, year over year.[1,2]

The .com and .net TLDs had a combined total of 165.2 million domain name registrations in the domain name base[3] at the end of the fourth quarter of 2020, an increase of 1.5 million domain name registrations, or 0.9 percent, compared to the third quarter of 2020. The .com and .net TLDs had a combined increase of 6.3 million domain name registrations, or 4.0 percent, year over year. As of Dec. 31, 2020, the .com domain name base totaled 151.8 million domain name registrations, and the .net domain name base totaled 13.4 million domain name registrations.

New .com and .net domain name registrations totaled 10.5 million at the end of the fourth quarter of 2020, compared to 10.3 million domain name registrations at the end of the fourth quarter of 2019.

Total new gTLD (ngTLD) domain name registrations were 26.0 million at the end of the fourth quarter of 2020, a decrease of 4.2 million domain name registrations, or 13.8 percent, compared to the third quarter of 2020. ngTLDs decreased by 3.3 million domain name registrations, or 11.2 percent, year over year.

TOP 10 LARGEST TLDs BY NUMBER OF REPORTED DOMAIN NAMES

Source: ZookNIC, Q4 2020; Verisign, Q4 2020; Centralized Zone Data Service, Q4 2020

151.8M	.com
24.7M	.cn
24.7M	.tk
16.7M	.de
13.4M	.net
10.9M	.uk
10.3M	.org
6.1M	.nl
5.7M	.ru
4.5M	.br
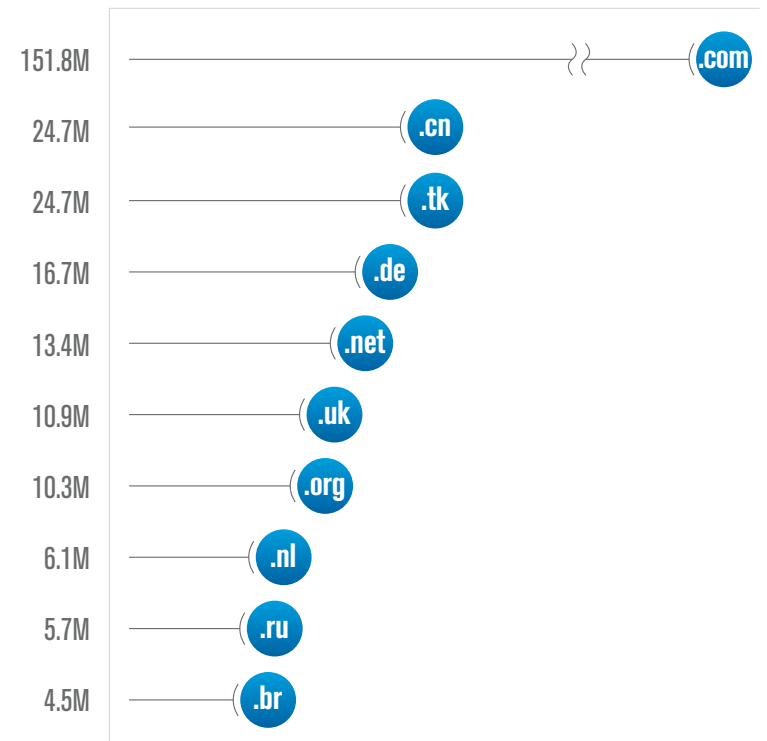
As of Dec. 31, 2020, the largest TLDs by number of reported domain names were .com, .cn, .tk, .de, .net, .uk, .org, .nl, .ru and .br.[1,2,4]
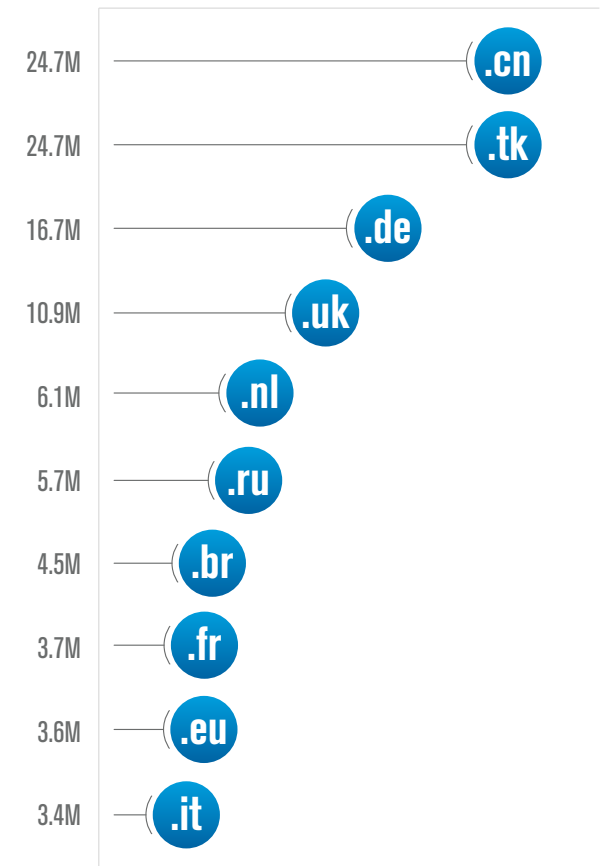
TOP 10 LARGEST ccTLDs BY NUMBER OF REPORTED DOMAIN NAMES

Total ccTLD domain name registrations were 158.9 million at the end of the fourth quarter of 2020, a decrease of 1.7 million domain name registrations, or 1.0 percent, compared to the third quarter of 2020.[1,2] ccTLDs increased by 1.3 million domain name registrations, or 0.8 percent, year over year.[1,2] Excluding .tk, ccTLD domain name registrations increased by 1.1 million in the fourth quarter of 2020, or 0.9 percent, compared to the third quarter of 2020. ccTLDs, excluding .tk, increased by 1.7 million domain name registrations, or 1.3 percent, year over year.
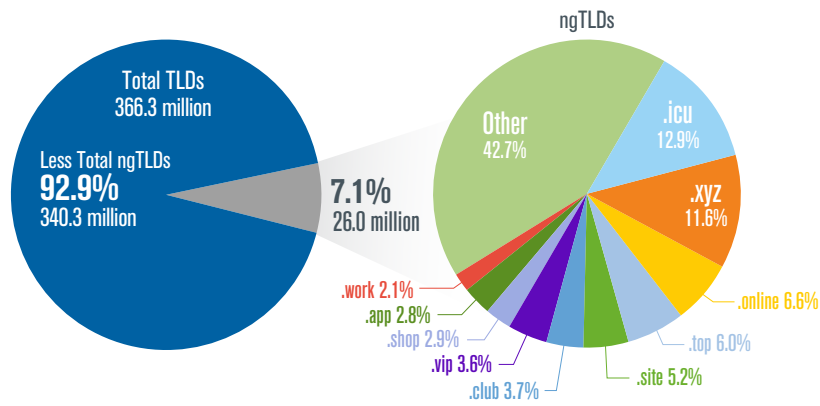
The top 10 ccTLDs, as of Dec. 31, 2020, were .cn, .tk, .de, .uk, .nl, .ru, .br, .fr, .eu and .it.[1,2] As of Dec. 31, 2020, there were 307 global ccTLD extensions delegated in the root zone, including IDNs, with the top 10 ccTLDs comprising 65.4 percent of all ccTLD domain name registrations.[1,2]

24.7M	.cn
24.7M	.tk
16.7M	.de
10.9M	.uk
6.1M	.nl
5.7M	.ru
4.5M	.br
3.7M	.fr
3.6M	.eu
3.4M	.it

NEW gTLDs AS PERCENTAGE OF TOTAL TLDs

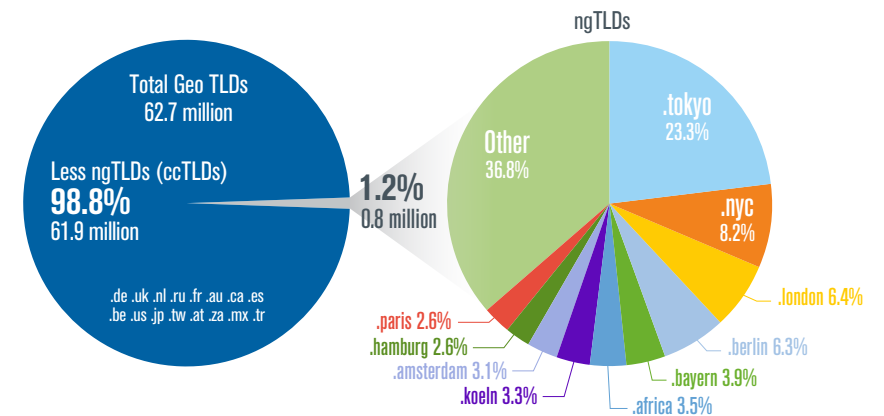Source: ZookNIC, Q4 2020; Verisign, Q4 2020; and Centralized Zone Data Service, Q4 2020

Total ngTLD domain name registrations were 26.0 million at the end of the fourth quarter of 2020, a decrease of 4.2 million domain name registrations, or 13.8 percent, compared to the third quarter of 2020. ngTLDs decreased by 3.3 million domain name registrations, or 11.2 percent, year over year. The top 10 ngTLDs represented 57.3 percent 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 7.1 percent, as well as the top 10 ngTLDs as a percentage of all ngTLD domain name registrations for the fourth quarter of 2020.

ngTLDs

Total TLDs
366.3 million

Less Total ngTLDs
92.9%
340.3 million

7.1%
26.0 million

Other 42.7%
.icu 12.9%
.xyz 11.6%
.online 6.6%
.top 6.0%
.site 5.2%
.club 3.7%
.vip 3.6%
.shop 2.9%
.app 2.8%
.work 2.1%

GEOGRAPHICAL ngTLDs AS PERCENTAGE OF TOTAL CORRESPONDING GEOGRAPHICAL TLDs

Source: ZookNIC, Q4 2020 and Centralized Zone Data Service, Q4 2020

As of Dec. 31, 2020, 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 (GA). The chart on the left summarizes the domain name registrations as of Dec. 31, 2020, 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.

ngTLDs

Total Geo TLDs
62.7 million

Less ngTLDs (ccTLDs)
98.8%
61.9 million

.de .uk .nl .ru .fr .au .ca .es
.be .us .jp .tw .at .za .mx .tr

1.2%
0.8 million

Other 36.8%
.tokyo 23.3%
.nyc 8.2%
.london 6.4%
.berlin 6.3%
.bayern 3.9%
.africa 3.5%
.koeln 3.3%
.amsterdam 3.1%
.hamburg 2.6%
.paris 2.6%

FROM THE VERISIGN BLOG / October – December 2020

Authenticated Resolution and Adaptive Resolution: Security and Navigational Enhancements to the Domain Name System

Two Verisign-developed technologies known as authenticated resolution and adaptive resolution give DNS name servers an important new role in improving a network's security and performance capabilities.

Cybersecurity Considerations in the Work-from-Home Era

Over the years, cybercriminals have grown more sophisticated, adapting to changing business practices and diversifying their approaches in non-traditional ways. Because of this, companies should educate employees on how to detect and avoid malicious websites to protect against threats.

Meeting the Evolving Challenges of COVID-19

When the COVID-19 pandemic struck earlier this year, it ushered in an immediate period of adjustment for us all. In response to the hardships that many in the community faced as a result of this pandemic, Verisign strengthened its outreach and support of local and statewide organizations focused on helping those in need.

Harnessing the Momentum of Women in Cybersecurity

Verisign is a proud supporter of the Uniting Women in Cyber (UWIC) organization and was a sponsor of the 2020 third annual UWIC symposium focused on women leaders in today's cybersecurity field. Heidi Austin, Verisign's senior director of IT service delivery, participated in a panel discussion in this virtual event, while executive vice president and chief security officer Danny McPherson received the organization's Cyber Champion Award.

A Balanced DNS Information Protection Strategy: Minimize at Root and TLD, Encrypt When Needed Elsewhere

"To encrypt or not to encrypt?" It's a question that Verisign has been considering for some time as part of our commitment to security, stability and resiliency of our DNS operations and the surrounding DNS ecosystem. In this piece, we explore why minimization at the root and top-level domain levels of DNS, and encrypting when needed elsewhere, is currently Verisign's recommended approach.

ARTICLE

INDUSTRY INSIGHTS: A BALANCED APPROACH TO DNS ENCRYPTION

By Burt Kaliski, Senior Vice President and Chief Technology Officer

As the Domain Name System (DNS) enters its fourth decade, it continues to evolve to meet the ever-changing needs of its users and operators. Originally designed to promote connection above all else, in recent years there has been an increased focus within the DNS on confidentiality. Notably, DNS encryption has recently come to the forefront and has sparked many conversations about how and when it should be used.

VERISIGN'S DNS ENCRYPTION RECOMMENDATION

Because of our role as a global provider of key internet infrastructure, Verisign is dedicated to a thorough and careful consideration of DNS encryption and related techniques.

We believe it is important to consider the operational needs of each level of the DNS separately. A "one size fits all" approach risks not fully meeting the unique security and operational considerations of all levels of the DNS, e.g. the root, top-level domain (TLD), second-level domain (SLD), and so forth.

Implementors have two main approaches for protecting the confidentiality of information exchanged within the DNS. **DNS encryption techniques** cryptographically conceal the information and reduce the risk of disclosure to outside parties who do not have the decryption key. Encryption can improve confidentiality and integrity by making it harder for an adversary to view or change data. Such techniques are bilateral: both parties involved in the exchange must implement them, and both therefore take on the operational risk of doing so.

Minimization techniques, in contrast, decrease the amount of information exchanged and reduce the risk of disclosing sensitive information to both outside and inside parties. These techniques are unilateral: only the sending party takes on additional functionality.

After significant research and collaboration within the DNS community, Verisign currently recommends using minimization techniques at the root- and TLD-server

levels and encrypting elsewhere when needed. Based on the current operational and cryptographic realities, this is a practical approach to balancing both confidentiality and availability of information exchanged within the DNS. A summary of this recommendation can be found in the table below.

Client-to-Resolver	Resolver-to-SLD and Below	Resolver-to-Root and TLD
Clients and resolvers should implement DNS encryption on this exchange, unless adequate protection is otherwise provided, e.g., as part of a network connection.	Resolvers and SLD servers should implement DNS encryption on their exchanges if sending sensitive full domain names, or client-specific information.	Resolvers should apply minimization techniques.

Table 1. Verisign's current recommendation for DNS confidentiality protections summarized

The rationale is straightforward: information exchanged at the root and TLD levels is by nature less sensitive, especially after minimization techniques are applied, yet is more critical to global navigation; the rest of the DNS below these levels depends on it. The risk-benefit tradeoff for DNS encryption is better justified in other parts of the DNS ecosystem where data is more sensitive and/or dependencies are more limited.

If this approach were followed, we could expect to see more deployment of minimization techniques on resolver-to-root and TLD exchanges; more deployment of DNS encryption, when needed, at the SLD levels and lower; and more deployment of DNS encryption on client-to-resolver exchanges. In all these deployments, the DNS will serve the same purpose as it already does with today's unencrypted exchanges: enabling general-purpose navigation to information and resources on the internet.

INDUSTRY INSIGHTS: A BALANCED APPROACH TO DNS ENCRYPTION (Cont.)

KEY CONSIDERATIONS IN VERISIGN'S DNS CONFIDENTIALITY PROTECTION RECOMMENDATION

When formulating this recommendation, we considered three key objectives, which are critical for any proposed information protection strategy:

- **Confidentiality**: does it protect information from disclosure?
- **Integrity**: does it protect information from modification?
- **Availability**: does it protect information from disruption?

Any solution must carefully balance these three elements. Furthermore, we factored in the risk versus benefit of any technique proposed to achieve these objectives, using a two-fold approach depicted in Figure 1 below.
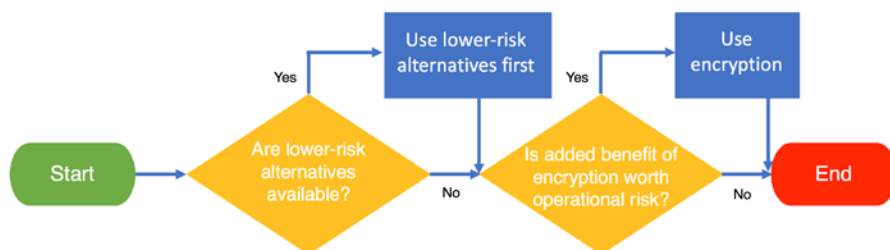

Figure 1. *Two-stage process for factoring in operational risk when determining how to address information protection objectives for a DNS exchange*

LOOKING TOWARD THE FUTURE: AUTHENTICATED RESOLUTION AND ADAPTIVE RESOLUTION

DNS encryption also brings two new capabilities that make it possible for the DNS to serve two new purposes. Both are based on concepts developed in Verisign's research program.

The first, called **authenticated resolution**, adds an enhanced security control point and brings the DNS in line with zero-trust principles. Authenticated resolution allows a requester to identify itself to a resolver or name server that supports DNS encryption. The resolver or name server can then return a response to the requester depending on whether the requester is authorized to receive the response, or ultimately, access the resources associated with the response.

The second, called **adaptive resolution**, adds a new navigation capability to the DNS. With adaptive resolution the requester provides information that the user has agreed to share with the web server to which the user is navigating, such as the user's preferences, the user's device, the information that the user is ultimately looking for or the action that the user wants to perform.[5] The resolver or name server then optimizes its response based on these additional details in order to both provide the best response and to minimize unnecessary subsequent transactions or computations.

Authenticated resolution and adaptive resolution can add to the functionality of the DNS at the places where DNS encryption is deployed, i.e. at the resolver-to-SLD (and below) and client-to-resolver exchanges, bringing new value to applications and end-users alike.

FINAL THOUGHTS

Visit the Verisign blog to read a more in-depth discussion of Verisign's views on DNS encryption, as well as to learn more about the potential applications of authenticated resolution and adaptive resolution.

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 307 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. https://www.businesswire.com/news/home/20131216006048/en/Freenom-Closes-3M-Series-Funding#.UxeUGNJDv9s.

2 The generic top-level domain (gTLD), 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.

5 Note that the resolver or name server implementing this technique is expected to be operated by the same entity as the web server, so the additional details wouldn't be provided to yet another party, they'd just be provided to the same party earlier in the process — and protected in transit via DNS encryption.

Verisign.com