THE DOMAIN NAME INDUSTRY BRIEF

VOLUME 18 – ISSUE 2
JUNE 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 first quarter of 2021 closed with 363.5 million domain name registrations across all top-level domains (TLDs), a decrease of 2.8 million domain name registrations, or 0.8%, compared to the fourth quarter of 2020.[1,2] Domain name registrations have decreased by 3.3 million, or 0.9%, year over year.[1,2]

Total country-code TLD (ccTLD) domain name registrations were 156.5 million at the end of the first quarter of 2021, a decrease of 2.4 million domain name registrations, or 1.5%, compared to the fourth quarter of 2020.[1,2] ccTLDs decreased by 0.9 million domain name registrations, or 0.6%, year over year.[1,2]

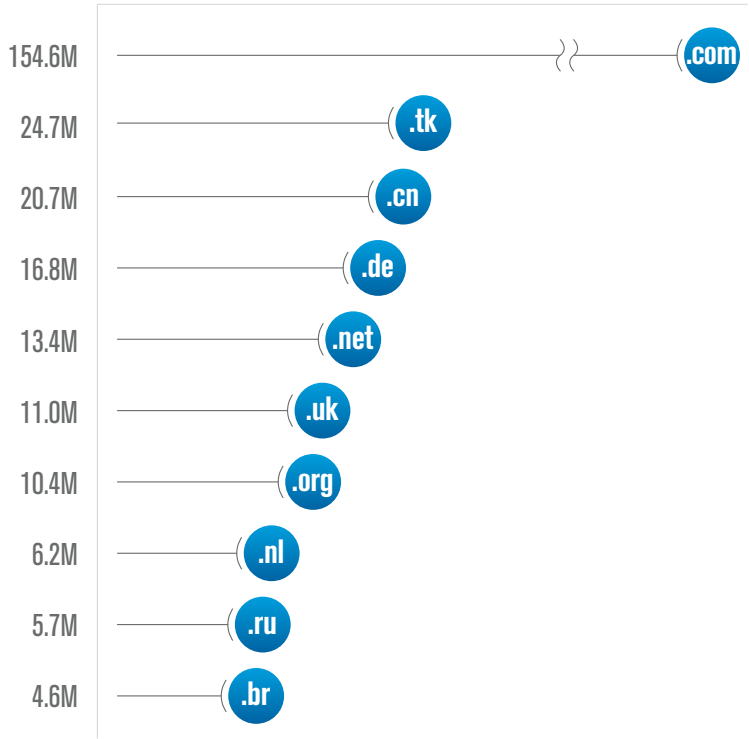
The .com and .net TLDs had a combined total of 168.0 million domain name registrations in the domain name base[3] at the end of the first quarter of 2021, an increase of 2.8 million domain name registrations, or 1.7%, compared to the fourth quarter of 2020. The .com and .net TLDs had a combined increase of 7.3 million domain name registrations, or 4.6%, year over year. As of March 31, 2021, the .com domain name base totaled 154.6 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 11.6 million at the end of the first quarter of 2021, compared to 10.0 million domain name registrations at the end of the first quarter of 2020.

Total new gTLD (ngTLD) domain name registrations were 22.8 million at the end of the first quarter of 2021, a decrease of 3.2 million domain name registrations, or 12.3%, compared to the fourth quarter of 2020. ngTLDs decreased by 9.5 million domain name registrations, or 29.3%, year over year.

TOP 10 LARGEST TLDs BY NUMBER OF REPORTED DOMAIN NAMES

Source: ZookNIC, Q1 2021; Verisign, Q1 2021; Centralized Zone Data Service, Q1 2021



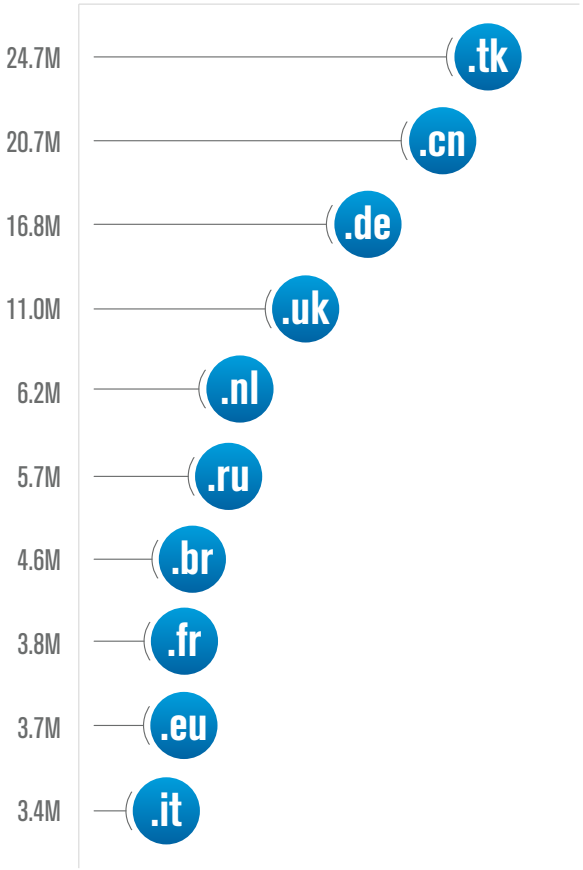
As of March 31, 2021, the largest TLDs by number of reported domain names were .com, .tk, .cn, .de, .net, .uk, .org, .nl, .ru and .br.[1,2,4]

TOP 10 LARGEST ccTLDs BY NUMBER OF REPORTED DOMAIN NAMES

Source: ZookNIC, Q1 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 156.5 million at the end of the first quarter of 2021, a decrease of 2.4 million domain name registrations, or 1.5%, compared to the fourth quarter of 2020.[1,2] ccTLDs decreased by 0.9 million domain name registrations, or 0.6%, year over year.[1,2] Excluding .tk, ccTLD domain name registrations decreased by 2.4 million in the first quarter of 2021, or 1.8%, compared to the fourth quarter of 2020. ccTLDs, excluding .tk, decreased by 0.5 million domain name registrations, or 0.4%, year over year.

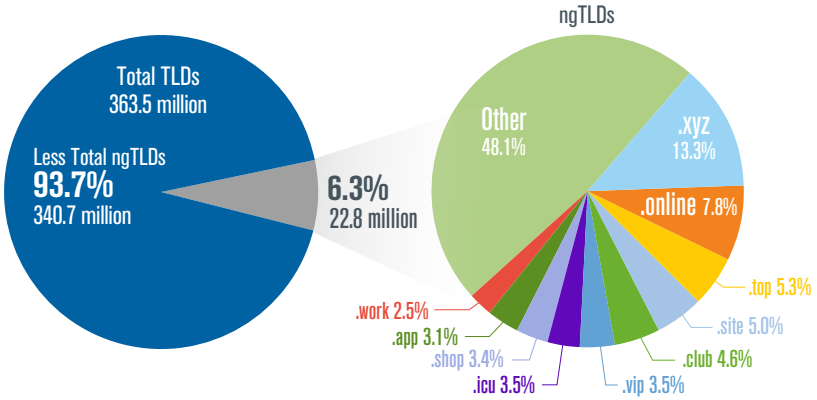
The top 10 ccTLDs, as of March 31, 2021, were .tk, .cn, .de, .uk, .nl, .ru, .br, .fr, .eu and .it.[1,2] As of March 31, 2021, there were 308 global ccTLD extensions delegated in the root zone, including IDNs, with the top 10 ccTLDs comprising 64.3% of all ccTLD domain name registrations.[1,2]



NEW gTLDs AS PERCENTAGE OF TOTAL TLDs

Source: ZookNIC, Q1 2021; Verisign, Q1 2021; and Centralized Zone Data Service, Q1 2021

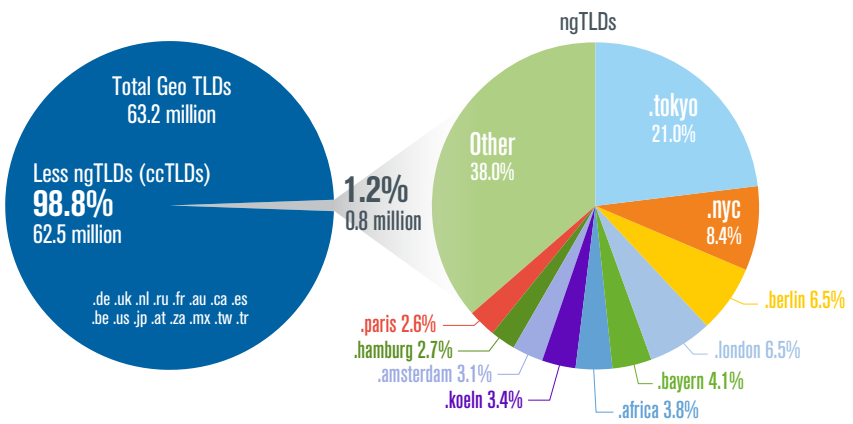
Total ngTLD domain name registrations were 22.8 million at the end of the first quarter of 2021, a decrease of 3.2 million domain name registrations, or 12.3%, compared to the fourth quarter of 2020. ngTLDs decreased by 9.5 million domain name registrations, or 29.3%, year over year. The top 10 ngTLDs represented 51.9% 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 6.3%, as well as the top 10 ngTLDs as a percentage of all ngTLD domain name registrations for the first quarter of 2021.



GEOGRAPHICAL ngTLDs AS PERCENTAGE OF TOTAL CORRESPONDING GEOGRAPHICAL TLDs

Source: ZookNIC, Q1 2021 and Centralized Zone Data Service, Q1 2021

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



FROM THE VERISIGN BLOG / January – March 2021

Chromium's Reduction of Root DNS Traffic

In late 2020, Verisign technologists discovered that more than 45% of total domain name system (DNS) traffic to the root servers was, at the time, the result of Chromium intranet redirection detection tests. In this blog, we provide an update on the latest development in Chromium responsiveness and its effect on network performance.

The Domain Name System: A Cryptographer's Perspective

Cryptography is part of almost every protocol, including the DNS. And from a cryptographer's perspective, there's so much more to the story than just encryption, as Verisign SVP and CTO explains in part one of his six-part series on DNS and cryptography.

Cryptographic Tools for Non-Existence in the Domain Name System: NSEC and NSEC3

Cryptographic approaches such as NSEC and NSEC3, which have been used by DNS servers when a domain name doesn't exist, increase the capabilities of the DNS.

Newer Cryptographic Advances for the Domain Name System: NSEC5 and Tokenized Queries

An experimental cryptographic approach known as NSEC5 and the related concept of tokenized queries could bring interesting new capabilities to the DNS.

FROM THE VERISIGN BLOG / January – March 2021 (Cont.)

Verisign Outreach Program Remediates Billions of Name Collision Queries

Verisign is committed to addressing name collision problems in the DNS, and its targeted outreach program continues to identify and remediate name collisions and minimize the attack surface exposed by name collisions.

Securing the DNS in a Post-Quantum World: New DNSSEC Algorithms on the Horizon

Post-quantum algorithms are among the newest developments in cryptography. When standardized, they could eventually be added into the DNS Security Extensions (DNSSEC) to help keep the DNS secure for the long term.

Securing the DNS in a Post-Quantum World: Hash-Based Signatures and Synthesized Zone Signing Keys

Research into concepts such as hash-based signatures and synthesized zone signing keys indicates that these techniques have the potential to enhance the security of the DNS if added into the DNSSEC.

Information Protection for the Domain Name System: Encryption and Minimization

Minimization techniques and encryption together give DNS designers additional tools for protecting DNS information — tools that when deployed carefully can balance between cryptographic and operational perspectives.

ARTICLE

INDUSTRY INSIGHTS: VERISIGN, ICANN AND INDUSTRY PARTNERS COLLABORATE TO COMBAT BOTNETS

By Matt Thomas and Duane Wessels, Distinguished Engineers

This article expands on observations of a botnet traffic group at various levels of the Domain Name System (DNS) hierarchy, presented at DNS-OARC 35.

Addressing DNS abuse and maintaining a healthy DNS ecosystem are important components of Verisign's commitment to being a responsible steward of the internet. We continuously engage with the Internet Corporation for Assigned Names and Numbers (ICANN) and other industry partners to help ensure the secure, stable and resilient operation of the DNS.

Based on recent telemetry data from Verisign's authoritative top-level domain (TLD) name servers, Verisign observed a widespread botnet responsible for a disproportionate amount of total global DNS queries – and, in coordination with several registrars, registries and ICANN, acted expeditiously to remediate it.

Just prior to Verisign taking action to remediate the botnet, upwards of 27.5 billion queries per day were being sent to Verisign's authoritative TLD name servers, accounting for roughly 10% of Verisign's total DNS traffic. That amount of query volume in most DNS environments would be considered a sustained distributed denial-of-service (DDoS) attack.

These queries were associated with a particular piece of malware that emerged in 2018, spreading throughout the internet to create a global botnet infrastructure. Botnets provide a substrate for malicious actors to theoretically perform all manner of malicious activity – executing DDoS attacks, exfiltrating data, sending spam, conducting phishing campaigns or even installing ransomware. This is the result of the malware's ability to download and execute any other type of payload the malicious actor desires.

Malware authors often apply various forms of evasion techniques to protect their botnets from being detected and remediated. A Domain Generation Algorithm (DGA) is an example of such an evasion technique.

DGAs are seen in various families of malware that periodically generate a number of domain names, which can be used as rendezvous points for botnet command-and-control servers. By using a DGA to build the list of domain names, the malicious actor makes it more difficult for security practitioners to identify what domain names will be used and when. Only by exhaustively reverse-engineering a piece of malware can the definitive set of domain names be ascertained.

The choices made by miscreants to tailor malware DGAs directly influences the DGAs' ability to evade detection. For instance, electing to use more TLDs and a large number of domain names in a given time period makes the malware's operation more difficult to disrupt; however, this approach also increases the amount of network noise, making it easier to identify anomalous traffic patterns by security and network teams. Likewise, a DGA that uses a limited number of TLDs and domain names will generate significantly less network noise but is more fragile and susceptible to remediation.

Botnets that implement DGA algorithms or utilize domain names clearly represent an "abuse of the DNS," opposed to other types of abuse that are executed "via the DNS," such as phishing. This is an important distinction the DNS community should consider as it continues to refine the scope of DNS abuse and how remediation of the various abuses can be effectuated.

The remediation of domain names used by botnets as rendezvous points poses numerous operational challenges and insights. The set of domain names needs to be identified and investigated to determine their current registration status. Risk assessments must be evaluated on registered domain names to determine if additional actions should be performed, such as sending registrar notifications, issuing requests to transfer domain names, adding Extensible Provisioning Protocol (EPP) hold statuses, altering delegation records, etc. There are also timing and coordination elements that must be balanced with external entities, such as ICANN, law enforcement, Computer Emergency Readiness Teams (CERTs) and contracted parties, including registrars

INDUSTRY INSIGHTS: VERISIGN, ICANN AND INDUSTRY PARTNERS COLLABORATE TO COMBAT BOTNETS (Cont.)

and registries. Other technical decisions also need to be considered, designed and deployed to achieve the desired remediation goal.

After coordinating with ICANN, and several registrars and registries, Verisign registered the remaining available botnet domain names and began a three-phase plan to sinkhole those domain names. Ultimately, this remediation effort would reduce the traffic sent to Verisign authoritative name servers and effectively eliminate the botnet's ability to use command-and-control domain names within Verisign-operated TLDs.

Figure 1 below shows the amount of botnet traffic Verisign authoritative name servers received prior to intervention, and throughout the process of registering, delegating and sinkholing the botnet domain names.

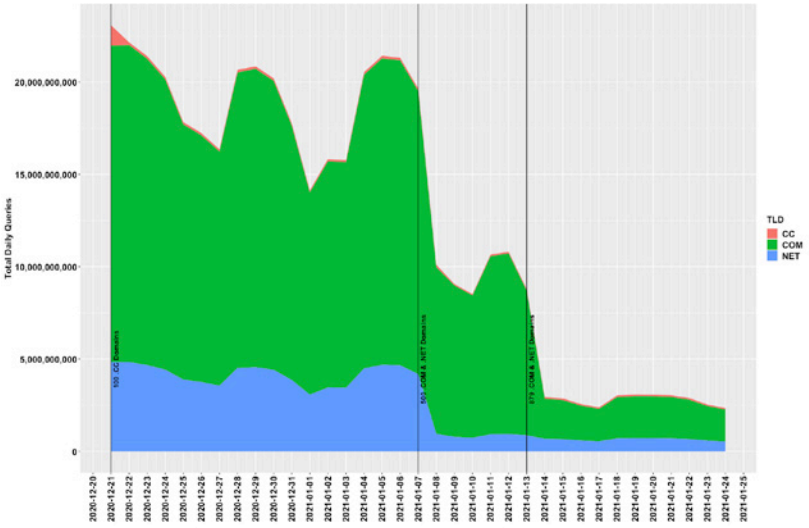


***Figure 1**. The botnet's DNS query volume at Verisign authoritative name servers*

Phase one was executed on Dec. 21, 2020, in which 100 .cc domain names were configured to resolve to Verisign-operated sinkhole servers. Subsequently, traffic at Verisign authoritative name servers quickly decreased. The second group of domain names contained 500 .com and .net domain names, which were sinkholed on Jan. 7, 2021. Again, traffic volume at Verisign authoritative name servers quickly decreased. The final group of 879 .com and .net domain names were sinkholed on Jan. 13, 2021. By the end of phase three, the cumulative DNS traffic reduction surpassed 25 billion queries per day. Verisign reserved approximately 10 percent of the botnet domain names to remain on serverHold as a placebo/control-group to better understand sinkholing effects as they relate to query volume at the child and parent zones. Verisign believes that sinkholing the remaining domain names would further reduce authoritative name server traffic by an additional one billion queries.

This botnet highlights the remarkable Pareto-like distribution of DNS query traffic, in which a few thousand domain names that span namespaces containing more than 165 million domain names, demand a vastly disproportionate amount of DNS resources.

What causes the amplification of DNS traffic volume for non-existent domain names to occur at the upper levels of the DNS hierarchy? Verisign is conducting a variety of measurements on the sinkholed botnet domain names to better understand the caching behavior of the resolver population. We are observing some interesting traffic changes at the TLD and root name servers when time to live (TTL) and response codes are altered at the sinkhole servers. Stay tuned.

In addition to remediating this botnet in late 2020 and into early 2021, Verisign extended its already four-year endeavor to combat the Avalanche botnet family. Since 2016, the Avalanche botnet had been significantly impacted due to actions taken by Verisign and an international consortium of law enforcement, academic and private organizations. However, many of the underlying Avalanche-compromised machines are still not remediated, and the threat from Avalanche could increase again if additional actions are not taken. To prevent this from happening, Verisign, in coordination with ICANN and other industry partners, is using a variety of tools to ensure Avalanche command-and-control domain names cannot be used in Verisign-operated TLDs.

Botnets are a persistent issue. And as long as they exist as a threat to the security, stability and resiliency of the DNS, cross-industry coordination and collaboration will continue to lie at the core of combating them.

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. 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.