

O DOSSIÊ SOBRE A INDÚSTRIA DE DOMÍNIOS NA INTERNET

VOLUME 17 – EDIÇÃO 4
NOVEMBRO DE 2020



VERISIGN®

DOSSIÊ SOBRE A INDÚSTRIA DE DOMÍNIOS NA INTERNET DA VERISIGN

Como provedora global de serviços de registro de nomes de domínio e infraestrutura na Internet, a Verisign analisa trimestralmente o estado do setor de nomes de domínio por meio de várias pesquisas analíticas e estatísticas. A Verisign oferece este dossiê para destacar as principais tendências em registros de nomes de domínio, além de importantes indicadores de desempenho e oportunidades de crescimento para analistas do setor, mídia e empresas.

RESUMO EXECUTIVO

O terceiro trimestre de 2020 foi encerrado com 370,7 milhões de registros de nomes de domínio em todos os domínios de nível superior (TLDs), um aumento de 0,6 milhão de registros de nomes de domínio (0,2%) comparado ao segundo trimestre de 2020.^{1,2} Os registros de nomes de domínio aumentaram em 10,8 milhões (3,0%) em relação ao ano anterior.^{1,2}

O total de registros de nomes de domínio TLD (ccTLD) de código de país foi de 160,6 milhões ao final do terceiro trimestre de 2020. Isso representa um aumento de 0,5 milhão de registros de nomes de domínio (0,3%), comparado ao segundo trimestre de 2020.^{1,2} Os ccTLDs diminuíram em 1,2 milhões de registros de nomes de domínio (0,7%), em relação ao ano anterior.^{1,2}

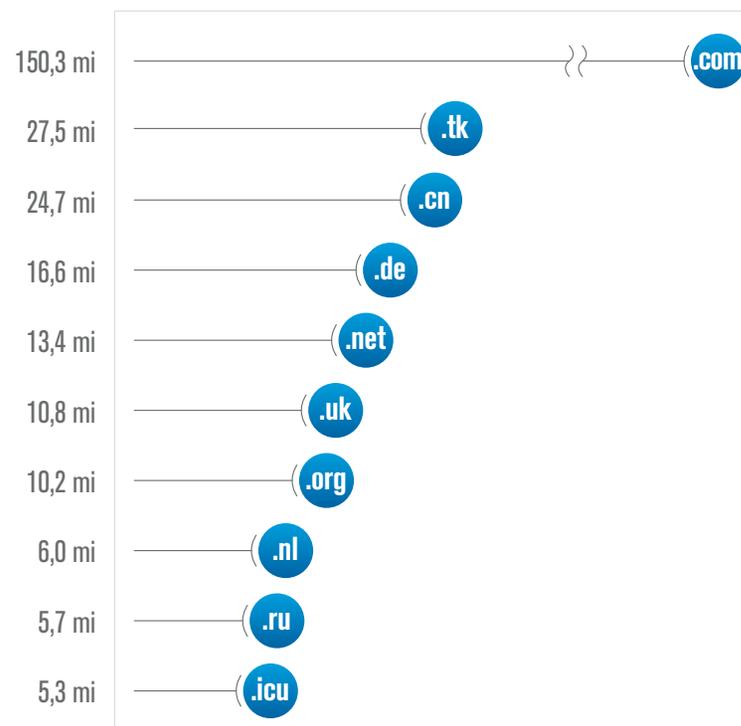
Os TLDs .com e .net tiveram um total de 163,7 milhões de registros de nomes de domínio em conjunto na base de nomes de domínio³ ao final do terceiro trimestre de 2020. Isso representa um aumento de 1,7 milhão de registros de nomes de domínio (1,0%) em relação ao segundo trimestre de 2020. Os TLDs .com e .net tiveram um aumento combinado de 6,3 milhões de registros de nomes de domínio (4,0%) em relação ao ano anterior. Em 30 de setembro de 2020, a base de nomes de domínio .com totalizou 150,3 milhões de registros de nomes de domínio, e a base de nomes de domínio .net totalizou 13,4 milhões de registros de nomes de domínio.

Os novos registros de nomes de domínio .com e .net totalizaram 10,9 milhões ao final do terceiro trimestre de 2020, comparados aos 9,9 milhões de registros de nomes de domínio ao final do terceiro trimestre de 2019.

O total de novos registros de nomes de domínio gTLD (ngTLD) foi de aproximadamente 30,2 milhões no final do terceiro trimestre de 2020, uma redução de 1,5 milhão de registros de nomes de domínio (4,7%) em comparação com o segundo trimestre de 2020. Os ngTLDs aumentaram em 6,2 milhões de domínios registros de nomes (25,8%) em relação ao ano anterior.

OS 10 MAIORES TLDs POR NÚMERO DE NOMES DE DOMÍNIO INFORMADOS

Fonte: ZookNIC, T3 de 2020; Verisign, T3 de 2020; Serviço de Dados de Zona Centralizado, T3 de 2020



A partir do dia 30 de setembro de 2020, os maiores TLDs por número de nomes de domínio informados eram .com, .tk, .cn, .de, .net, .uk, .org, .nl, .ru e .icu.^{1,2,4}



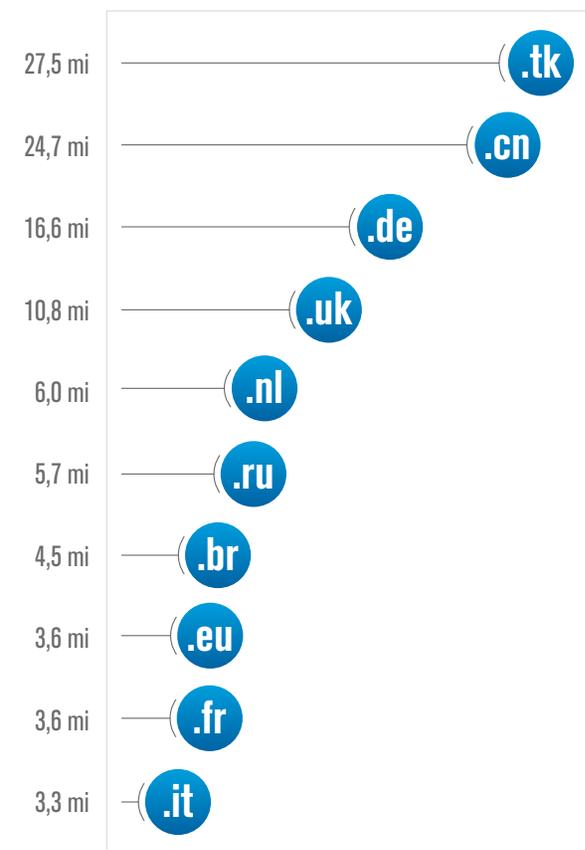
OS MAIORES ccTLDs POR NÚMERO DE NOMES DE DOMÍNIO INFORMADOS

Fonte: ZookNIC, T3 de 2020

Para obter mais informações sobre a metodologia do *Dossiê sobre a indústria de domínios na Internet*, consulte a última página deste dossiê.

O total de registros de nomes de domínio ccTLD foi de 160,6 milhões ao final do terceiro trimestre de 2020. Isso representa um aumento de 0,5 milhão de registros de nomes de domínio (0,3%) comparado ao segundo trimestre de 2020.^{1,2} Os ccTLDs diminuíram em 1,2 milhão de registros de nomes de domínio (0,7%) em relação ao ano anterior.^{1,2} Sem incluir .tk, os registros de nome de domínio ccTLD aumentaram 0,5 milhão no terceiro trimestre de 2020 (0,4%) comparado ao segundo trimestre de 2020. Os ccTLDs, excluindo .tk, diminuíram em 3,6 milhões de registros de nome de domínio (2,6%), em relação ao ano anterior.

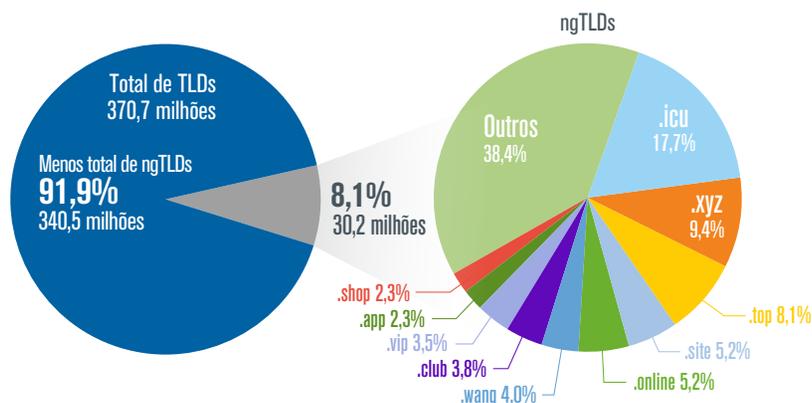
Os 10 maiores ccTLDs, em 30 de setembro de 2020, eram .tk, .cn, .de, .uk, .nl, .ru, .br, .eu, .fr e .it.^{1,2} Em 30 de setembro de 2020, havia 307 extensões globais de ccTLDs delegadas na zona raiz, incluindo nomes de domínio internacionalizados (IDNs), com os 10 maiores ccTLDs compreendendo 66,2% de todos os registros de nomes de domínio ccTLD.^{1,2}



NOVOS gTLDs COMO PORCENTAGEM DO TOTAL DE TLDs

Fonte: ZookNIC, T3 de 2020; Verisign, T3 de 2020; e Serviço de Dados de Zona Centralizado, T3 de 2020

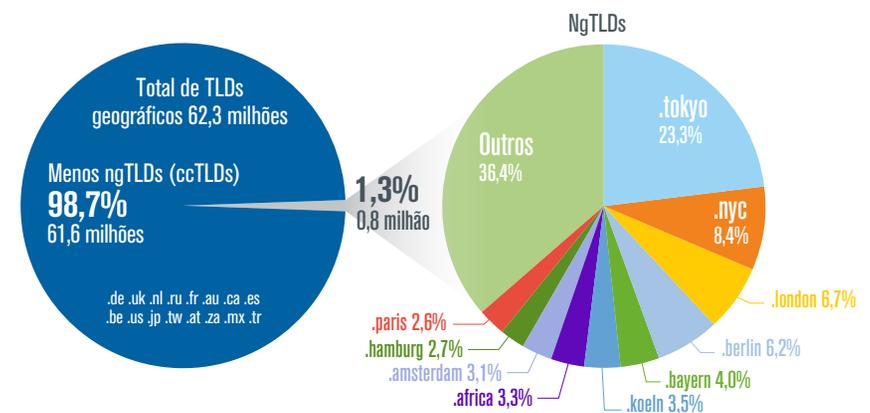
O total de registros de nomes de domínio ngTLD foi de 30,2 milhões no final do terceiro trimestre de 2020, uma redução de 1,5 milhão de registros de nomes de domínio (4,7%) em comparação com o segundo trimestre de 2020. Os ngTLDs aumentaram em 6,2 milhões de registros de nomes de domínio (25,8%) em relação ao ano anterior. Os 10 principais ngTLDs representaram 61,6% de todos os registros de nomes de domínio ngTLD. O gráfico a seguir mostra os registros de nomes de domínio ngTLD como uma porcentagem do total de registros de nomes de domínio TLD, dos quais representam 8,1%, assim como os 10 principais ngTLDs como uma porcentagem de todos os registros de nomes de domínio ngTLD para o terceiro trimestre de 2020.



PORCENTAGEM DE ngTLDs GEOGRÁFICOS EM RELAÇÃO AO TOTAL CORRESPONDENTE DE TLDs GEOGRÁFICOS

Fonte: ZookNIC, T3 2020 e Serviço de Dados de Zona Centralizado, T3 2020

Em 30 de setembro de 2020, havia 47 ngTLDs delegados que atendiam aos seguintes critérios: 1) ter um foco geográfico e 2) ter mais de 1.000 registros de nomes de domínio desde que entraram na disponibilidade geral. O gráfico à esquerda resume os registros de nomes de domínio em 30 de setembro de 2020, para os ccTLDs listados e os ngTLDs geográficos correspondentes dentro da mesma região geográfica. Além disso, o gráfico à direita apresenta a porcentagem dos 10 principais ngTLDs geográficos em relação ao total de TLDs geográficos.





NOTÍCIA NO BLOG DA VERISIGN /Julho a setembro de 2020



Combatendo a venda ilegal de opioides na Internet na era da COVID-19

Um programa piloto lançado na primavera de 2020 forneceu uma estrutura para a colaboração entre a Verisign, a Food and Drug Administration (FDA) e a National Telecommunications and Information Administration (NTIA).



DNS: um componente essencial da computação em nuvem

A evolução da Internet está ancorada no fenômeno da substituição de tecnologias mais antigas por novas tecnologias. Mas a evolução da tecnologia pode significar tanto construir sobre o que já existe quanto destruir inovações passadas. Na verdade, o surgimento da computação em nuvem foi impulsionado pela extensão de um componente subjacente improvável: o sistema de nomes de domínio (DNS) global com mais de 30 anos de existência.



Impacto do Chromium no tráfego do DNS raiz

O Chromium é um projeto de software de código aberto que forma a base do navegador Chrome da Google, entre outros produtos de navegador. Os tecnólogos da Verisign exploram como um dos recursos do Chromium, destinado a identificar se uma rede está tentando “sequestrar” resultados de domínio inexistentes, afeta o tráfego do DNS raiz. A análise revela que as consultas de sondagem do Chromium representam atualmente quase metade de todo o tráfego do servidor raiz do DNS.



Maximizando a minimização de Qname: um novo capítulo na evolução do protocolo DNS

A minimização de Qname é uma etapa simples, mas inovadora na evolução da implementação do protocolo DNS. É um modo fundamental de reduzir a sensibilidade dos dados do DNS trocados entre os resolvedores e os servidores raiz e de domínio de nível superior (TLD), bem como quaisquer outros servidores de nomes antes do último na cadeia.

CONSIDERAÇÕES SOBRE SEGURANÇA CIBERNÉTICA NA ERA DO TRABALHO EM CASA

Por Yong Kim, Vice-Presidente de Pesquisa e Estratégia Cibernética

A Verisign está profundamente comprometida em proteger nossa infraestrutura de Internet fundamental contra potenciais ameaças de segurança cibernética e em se manter atualizada sobre as mudanças no cenário cibernético.

Com o passar dos anos, os criminosos cibernéticos ficaram mais sofisticados, adaptando-se às mudanças nas práticas de negócios e diversificando suas abordagens de maneiras não tradicionais. Vimos ameaças à segurança continuarem evoluindo em 2020, à medida que muitas empresas mudaram para uma postura de trabalhar em casa devido à pandemia de COVID-19. Por exemplo, o fenômeno das videoconferências e sessões de aprendizado on-line “bombardeando pelo Zoom” não tinha sido um problema generalizado até que, de repente, se tornou um.

À medida que mais pessoas começaram a acessar aplicativos e arquivos da empresa em suas redes domésticas, os departamentos de TI implementaram novas ferramentas e definiram novas políticas para encontrar o equilíbrio certo entre proteger os ativos da empresa e informações confidenciais, e permitir que os funcionários sejam tão produtivos em casa quanto seriam no escritório. Mesmo o salto exponencial no uso de [impressoras em rede doméstica](#), que pode ou não ser devidamente protegido, representou uma nova questão de segurança para algumas equipes de TI corporativas.

Um aumento nos golpes de phishing acompanhou essa mudança nos padrões de trabalho. Cerca de um mês depois que grande parte da força de trabalho global começou a trabalhar em casa em grande número, o Federal Bureau of Investigation (FBI) relatou um [aumento de 300% a 400%](#) no recebimento de reclamações de segurança cibernética pelo Internet Crime Complaint Center (IC3) a cada dia. [De acordo com a Organização Internacional de Polícia Criminal \(Interpol\)](#), “[dos] ciber-golpes globais, 59% ocorrem na forma de spear phishing”. Essas campanhas de phishing visavam uma variedade de setores, como saúde e agências governamentais, imitando especialistas em saúde ou instituições de caridade relacionadas à COVID.

Medidas proativas podem ajudar as empresas a melhorar a higiene da segurança cibernética e se proteger contra golpes de phishing. Uma dessas medidas para as empresas é concentrar parte de seus esforços em educar os funcionários sobre como detectar e evitar sites maliciosos em e-mails de phishing. As empresas podem começar desenvolvendo a compreensão dos funcionários sobre como identificar o domínio de destino de um URL (Uniform Resource Locator – comumente referido como “links”) incorporado em um e-mail que pode ser malicioso. Os URLs podem ser complexos e confusos e os criminosos cibernéticos, que estão bem cientes dessa complexidade, costumam usar táticas enganosas dentro dos URLs para mascarar o domínio de destino malicioso. As empresas podem tomar medidas proativas para informar seus funcionários sobre essas táticas enganosas e ajudá-los a evitar sites maliciosos. Algumas das táticas mais comuns são descritas na Tabela 1 abaixo.

Tática	O que é?
Combosquatting	Adicionar palavras como “seguro”, “login” ou “conta” a um nome de domínio familiar para induzir os usuários a pensar que ele está afiliado ao nome de domínio conhecido.
Typosquatting	Usar nomes de domínio que se assemelham a um nome familiar, mas incorporam erros tipográficos comuns, como inverter letras, omitir ou adicionar um caractere.
Levelsquatting	Usar nomes ou nomes de domínio familiares como parte de um subdomínio dentro de um URL, dificultando a descoberta do domínio de destino real.
Ataques por homógrafos	Usar nomes de domínio homógrafos ou semelhantes, como substituir o “l” maiúsculo ou o número “1” onde deveria ter sido usado um “L” minúsculo, ou usar “é” em vez de “e”.

CONSIDERAÇÕES SOBRE SEGURANÇA CIBERNÉTICA NA ERA DO TRABALHO EM CASA (Cont.)

Tática	O que é?
Domínios posicionados inadequadamente	Inserir nomes de domínio familiares dentro do URL como uma forma de adicionar um nome de domínio familiar a um URL de aparência complexa. O nome de domínio familiar pode ser encontrado em um caminho (após “/”), como parte dos parâmetros adicionais (após “?”), como um identificador de âncora/fragmento (após “#”) ou nas credenciais HTTP (antes de “@”).
Caracteres codificados por URL	Colocar caracteres codificados por URL (%[code]), que às vezes são usados em parâmetros de URL, no próprio nome de domínio.

Tabela 1. Táticas comuns usadas por criminosos cibernéticos para mascarar o domínio de destino.

Ensinar os usuários a encontrar e compreender a parte do domínio do URL pode ter efeitos duradouros e positivos na capacidade de uma organização de evitar links de phishing. Ao fornecer aos funcionários (e suas famílias) essas informações básicas, as empresas podem se proteger melhor contra problemas de segurança cibernética, como comprometimento de redes, perdas financeiras e violações de dados.

Para saber mais sobre o que você pode fazer para proteger a si mesmo e sua empresa contra possíveis ameaças cibernéticas, consulte a campanha on-line STOP. THINK. CONNECT. em <https://www.stophinkconnect.org>. STOP. THINK. CONNECT. é uma campanha global de conscientização sobre segurança on-line liderada pela National Cyber Security Alliance e em parceria com o Anti-Phishing Working Group para ajudar todos os cidadãos digitais a ficarem mais seguros na Internet.



VERISIGN®

SOBRE A VERISIGN

A Verisign, fornecedora global de serviços de registro de nomes de domínio e infraestrutura da Internet, permite a navegação na Internet para vários dos nomes de domínio mais reconhecidos do mundo. A Verisign permite a segurança, estabilidade e flexibilidade dos principais serviços e infraestrutura da Internet, inclusive a prestação de serviços de manutenção da zona raiz, a operação de dois dos 13 servidores raiz da Internet e a prestação de serviços de registro e resolução autorizada para os domínios de primeiro nível .com e .net, usados pela maior parte do comércio eletrônico global. Para saber mais sobre o que significa a tecnologia Verisign, acesse Verisign.com.

SAIBA MAIS

Para ver a média de consultas diárias processadas pela Verisign, acesse a seção "O que fazemos" em Verisign.com.⁵ Para acessar os arquivos do *Dossiê sobre a indústria de domínios na Internet*, visite Verisign.com/DNIBArchives. Envie seus comentários ou perguntas para DomainBrief@verisign.com.

METODOLOGIA

Os dados apresentados neste dossiê, incluindo as métricas de trimestre a trimestre e ano a ano, refletem as informações disponíveis para a Verisign no ato de elaboração deste dossiê, e podem incorporar alterações e ajustes aos períodos informados anteriormente, com base em informações adicionais desde a data dos relatórios anteriores, para refletir de maneira mais precisa a taxa de crescimento de registros de nomes de domínio. Além disso, os dados disponíveis para este dossiê podem não incluir os dados para todas as 307 extensões ccTLD delegadas para a zona raiz, e inclui apenas os dados disponíveis no momento da preparação deste dossiê.

Para os dados gTLD e ccTLD citados com o ZookNIC como fonte, a análise do ZookNIC utiliza a comparação das mudanças no arquivo da zona raiz dos nomes de domínio, complementadas por dados Whois em um modelo estatístico de nomes de domínio, que lista a empresa de registro de domínios responsável por um nome de domínio em particular e a localização do solicitante do registro. Os dados têm uma margem de erro com base no tamanho da amostra e do mercado. Os dados ccTLD são baseados em análises de arquivos de zona raiz. Para obter mais informações, acesse ZookNIC.com.

1 A(s) figura(s) inclui(em) nomes de domínio no ccTLD .tk. .tk é um ccTLD gratuito que oferece nomes de domínio gratuitos para indivíduos e empresas. A receita é gerada ao monetizar os nomes de domínio expirados. Os nomes de domínio que não são mais usados pelo solicitante do registro ou que tenham expirado são pegos de volta pelo registro e o tráfego residual é vendido para redes de anúncios. Assim, não há nomes de domínio .tk excluídos. <https://www.businesswire.com/news/home/20131216006048/en/Freedom-Closes-3M-Series-Funding#.UxeUGNJDv9s>.

2 Os dados de domínio de primeiro nível genérico (gTLD) e ccTLD citados neste dossiê: (i) incluem nomes de domínio internacionalizados (IDNs) ccTLD; (ii) são uma estimativa válida até a data em que este dossiê foi elaborado; e (iii) estão sujeitos a alterações à medida que se recebem dados mais completos. Alguns números neste dossiê podem refletir o arredondamento padrão.

3 A base dos nomes de domínio é a zona ativa mais o número de nomes de domínio registrados, mas não configurados, para o uso no respectivo arquivo de zona TLD, mais o número de nomes de domínio que estão em modo de espera no servidor ou no cliente. O número de registros de nomes de domínio .com e .net corresponde ao relatado nos arquivos mais recentes da Verisign na SEC.

4 A linha de interrupção indica que a linha .com foi reduzida para considerações de visualização.

5 A seção "O que fazemos" está localizada no site Verisign.com, sob a aba "Sobre a Verisign" e sob a subaba "Visão geral".

Verisign.com