Newly Registered Domains V2 (NRD2) Top ccTLD Coverage Increased by 154% in 2023

Posted on December 12, 2023

WhoisXML API continues to improve its products and services as part of its commitment to a safer and more transparent Internet through the delivery of high-quality and reliable domain, IP, and DNS intelligence sources.

Among our most recent developments is the massive increase in the country-code top-level domain (ccTLD) coverage of the Newly Registered Domains V2 (NRD2) Data Feed. Specifically, we recorded a 153.95% increase in the number of domain activity for the top 10 ccTLDs in 2023 compared to 2022.

Compiling ccTLD domain data is generally challenging because of the various entities and requirements involved in the domain record collection and aggregation process, making this growth in coverage a noteworthy achievement for users seeking data reliability and comprehensiveness.

The Importance of ccTLD Domain Data

Over the years, registrants of new domain names started transitioning away from the usual .com, .net, and other generic TLD (gTLD) extensions. While gTLDs continue to be widely used in domain registrations, ccTLDs are also becoming increasingly popular due to localization strategies and various initiatives encouraging people to register domains with their local ccTLDs.

It is essential to keep an eye on the growing volume of ccTLD registrations because, like otherTLD types, ccTLD domains can and are being used for various purposes, both with legitimate and malicious intent.

Incorporating ccTLD domains into your NRD tracking efforts is, therefore, critical to enable several business and cybersecurity processes.

Cybersecurity Use Cases of ccTLD Domain Data

Among the many uses of ccTLD data in cybersecurity are:

- **Domain name filtering:** Blocking access to suspicious domain names sporting ccTLDs can help prevent users from falling victim to phishing attacks and other forms of cybercrime.
- **Mapping cybercrime networks:** Analyzing the geographical distribution of suspicious domains sporting ccTLDs can hint at the origin and scope of possible cybercrime networks.
- **Collaborating with international partners:** Sharing ccTLD data with international partners can effectively help law enforcement agencies and cybersecurity professionals combat cybercrime across borders.
- **Monitoring botnet activity:** Tracking ccTLD domain registrations for signs of botnet involvement can allow security researchers and teams to identify and disrupt botnet command-and-control (C&C) servers before they can cause significant harm.
- **Correlating ccTLD data with other threat intelligence:** Combining ccTLD data with other intelligence sources, such as blocklists and malware reports, can help cybersecurity professionals identify emerging threats and track cybercriminal activity.

Economic and Business Use Cases of ccTLD Domain Data

Aside from cybersecurity, ccTLD data can also inform and empower several business and economic processes, including:

- **Domain name valuation:** Analyzing the ccTLD registration volume can help registrars, domain name investors, and other entities estimate the potential value of specific domain names.
- **Brand protection:** Tracking the ownership and other details of ccTLD domains can support the identification of potential legal or intellectual property issues.
- **Launching targeted advertising campaigns:** Utilizing ccTLD data can be useful to tailor online advertising campaigns to specific countries and regions, ensuring maximum reach and effectiveness.
- **Economic analysis:** Gaining insights from the registration trends of specific ccTLDs can help gauge economic growth and Internet penetration rates in different countries.

—

Access to ccTLD data is available through our Newly Registered Domains V2 (NRD2) Enterprise and Ultimate packages.

You may download NRD data feed samples for free here or contact us for more information about how new domain intelligence can empower your processes and solutions.