2023年9月域名事件重点回顾

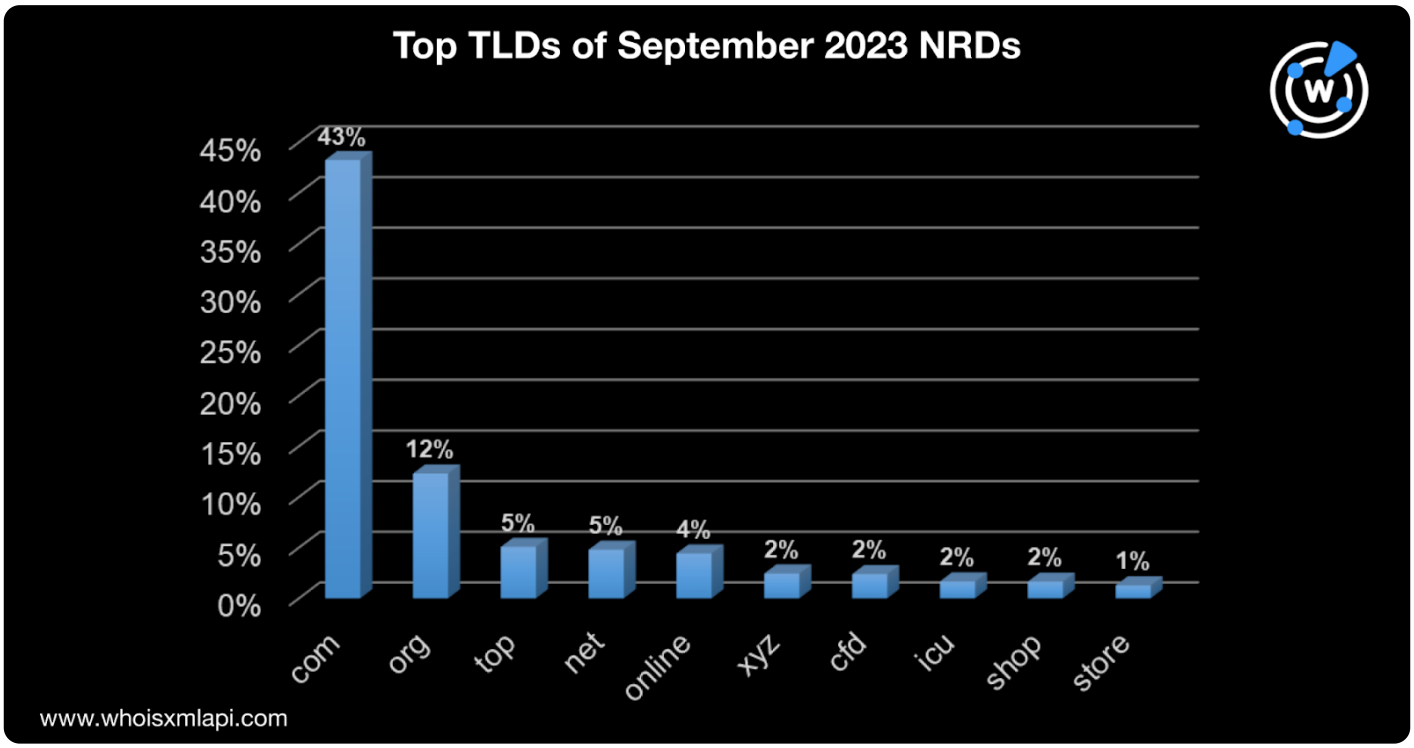
发布于 November 1, 2023

2023年9月1日-30日期间域名注册约数百万，WhoisXML
API分析师从中随机选取了30,000个域名作为样本进行分析，研究这些域名的注册国家、注册商和顶级域情

9月新注册域名详情

顶级域分布情况

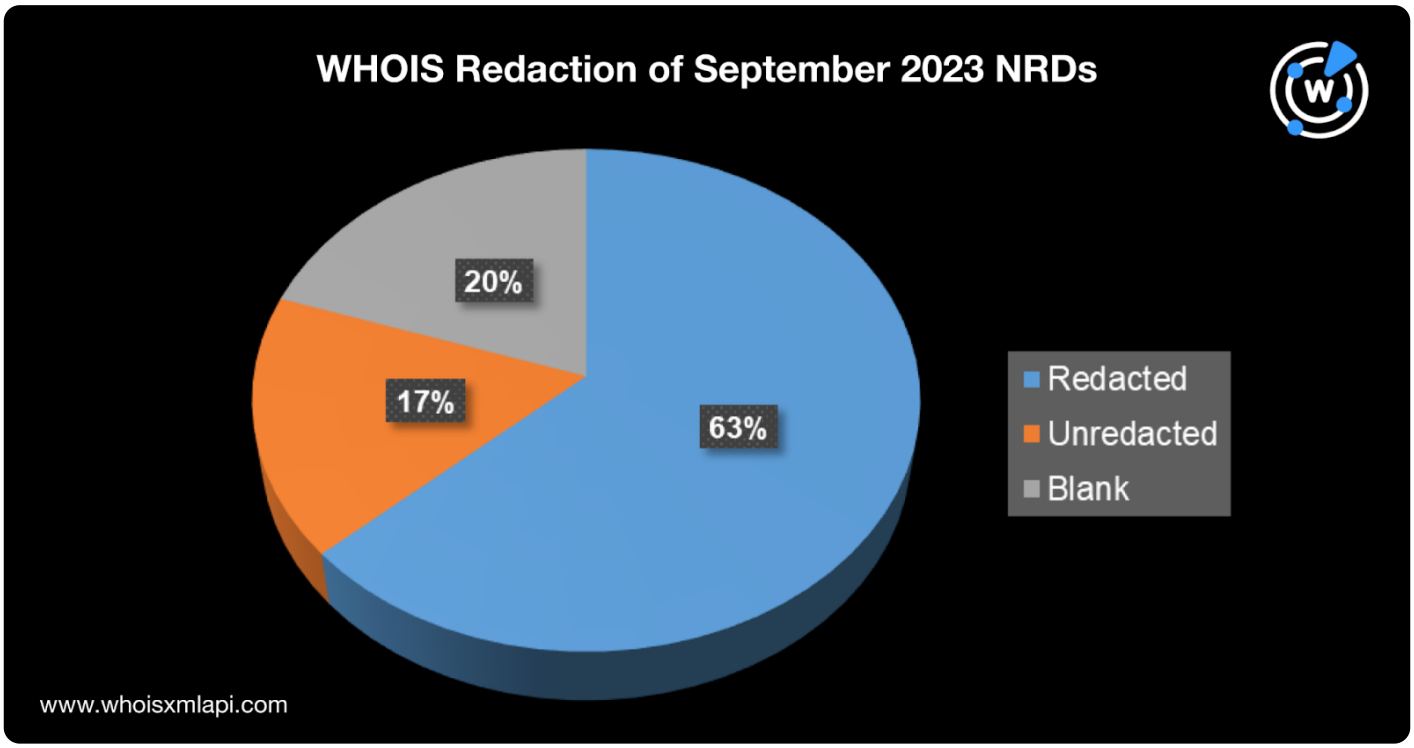
9月份中排名前十的顶级域名和前几月的情况保持基本一直，.com顶级域后缀仍然是使用最多的，占域名注
.cfd, .icu, 和.shop (分别占比2%) 以及 .store (占比1%)。



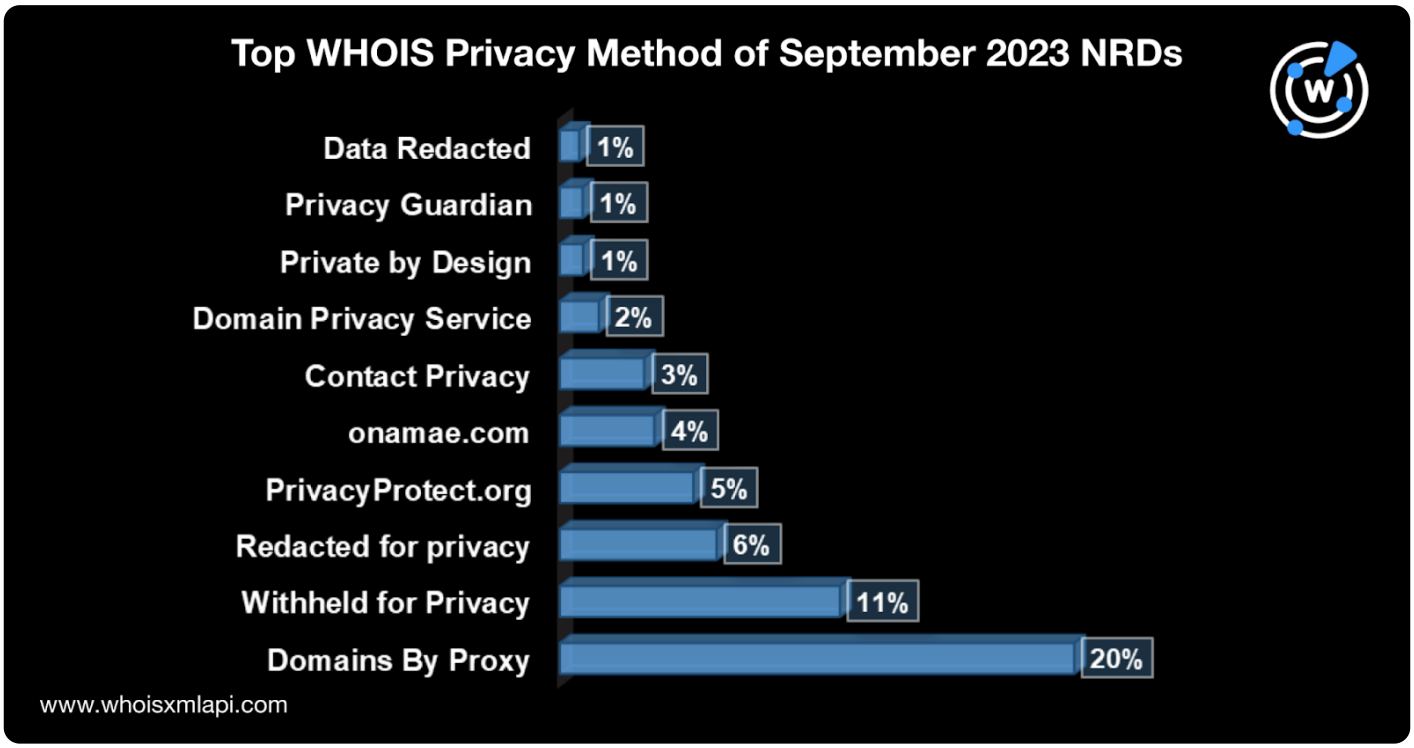
排名前十的顶级域占新注册域名总量的79%，剩余的域名则分布在630多个顶级域中。

WHOIS 数据编辑

约有63%的新注册域名使用了WHOIS数据编辑服务，只有17%的域名则公开其注册机构，而约20%的域名则



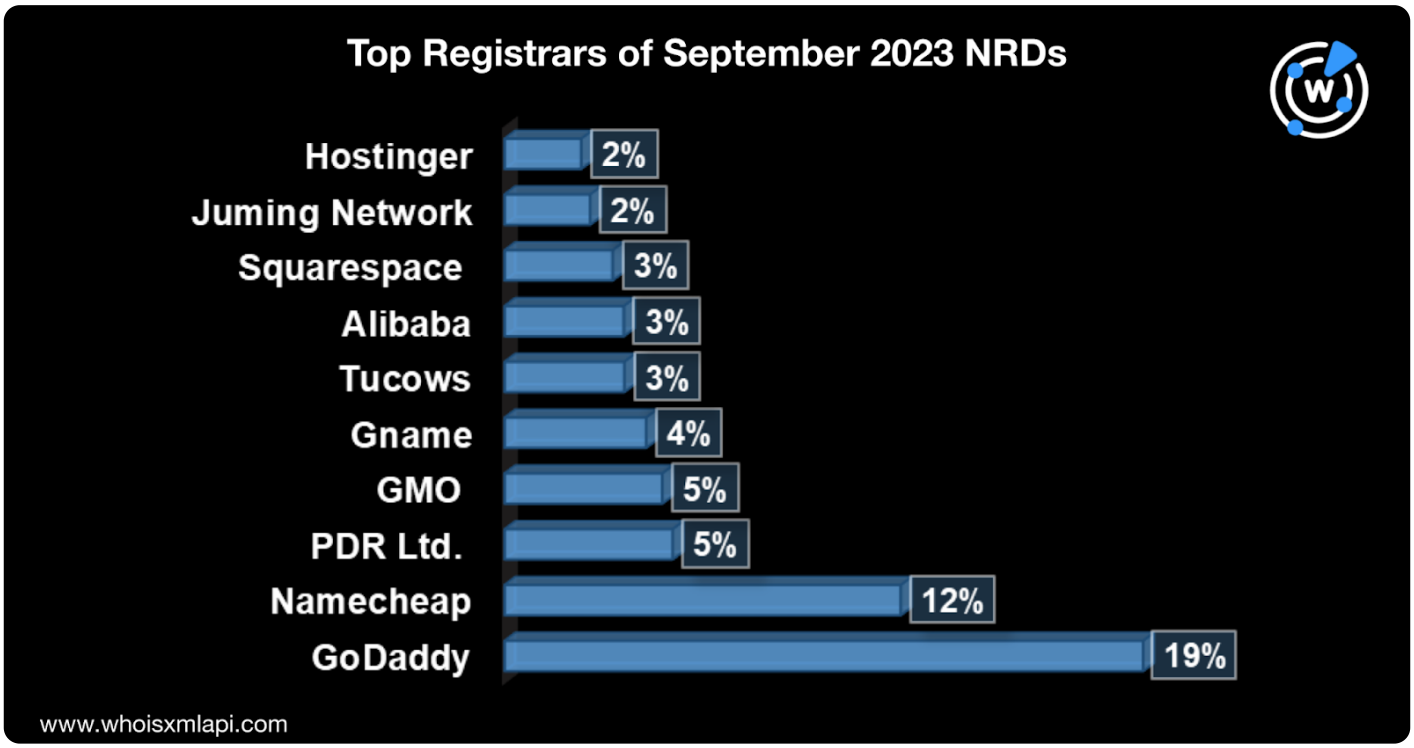
Domains By Proxy依然是最受欢迎的隐私编辑服务提供商，占新注册域名注册量的20%，紧随其后的是Withheld for Privacy，占比11%；Privacy Protect，占比5%，Onamae，占比4%，Contact Privacy占比3%，Domain Privacy Service占比2%，Private by Design占比1%，以及 Privacy Guardian占比1%。



一些新注册域名的注册机构一栏还包括一些信息，如“私人”、“隐私编辑保护”、“数据编辑”和“GDP

注册商分布

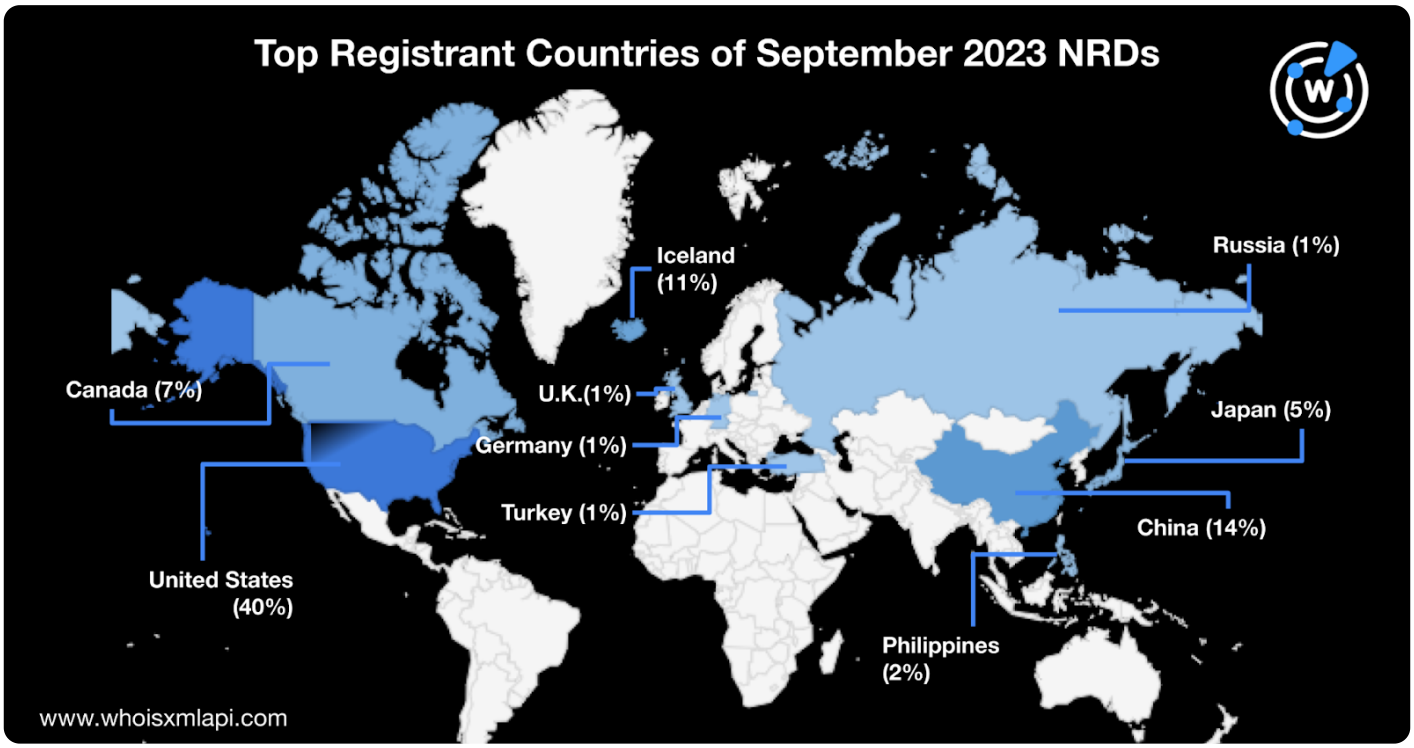
9月份的注册商排名中，GoDaddy独占鳌头，占新域名注册总量的19%。Namecheap排名第二，占比约为1
Ltd.和GMO Internet，分别为5%，Gname占比4%，Tucows, Alibaba,
和Squarespace分别为3%，Juming Network和Hostinger依旧排在前十名之内，占比分别为2%。



排名前十的注册商占据了域名注册总量的58%，剩余的域名则分布在580多家其他的注册商中。

排名领先的注册国家

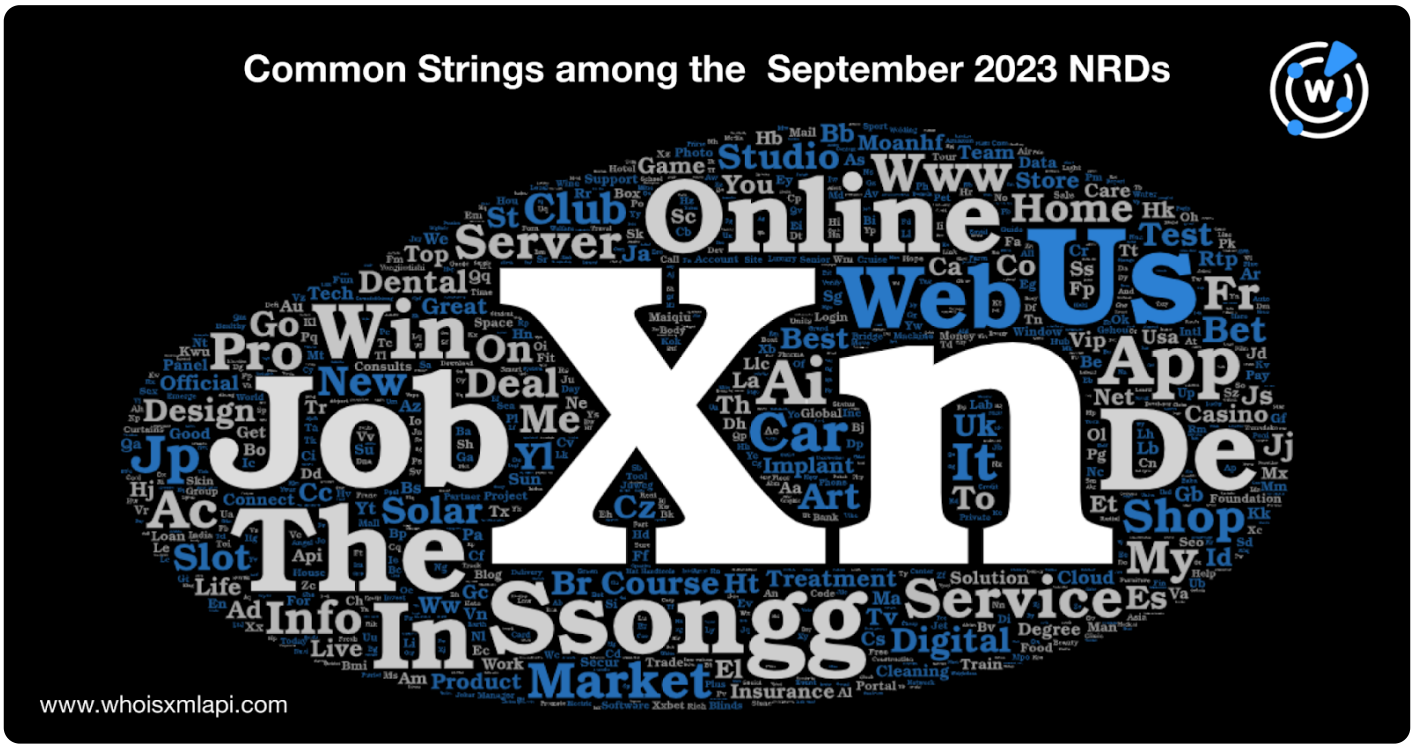
在9月份的新域名注册中，美国依旧是排名领先的国家（占比40%），中国和冰岛紧随其后，分别占14% 和
11%。剩余排名前十的注册国家依次为加拿大（7%）、日本（5%）、菲律宾（2%），俄罗斯、英国、德国



排名前十的注册国家占域名注册总量的83%，剩下的域名则分布在115多个其他国家中。

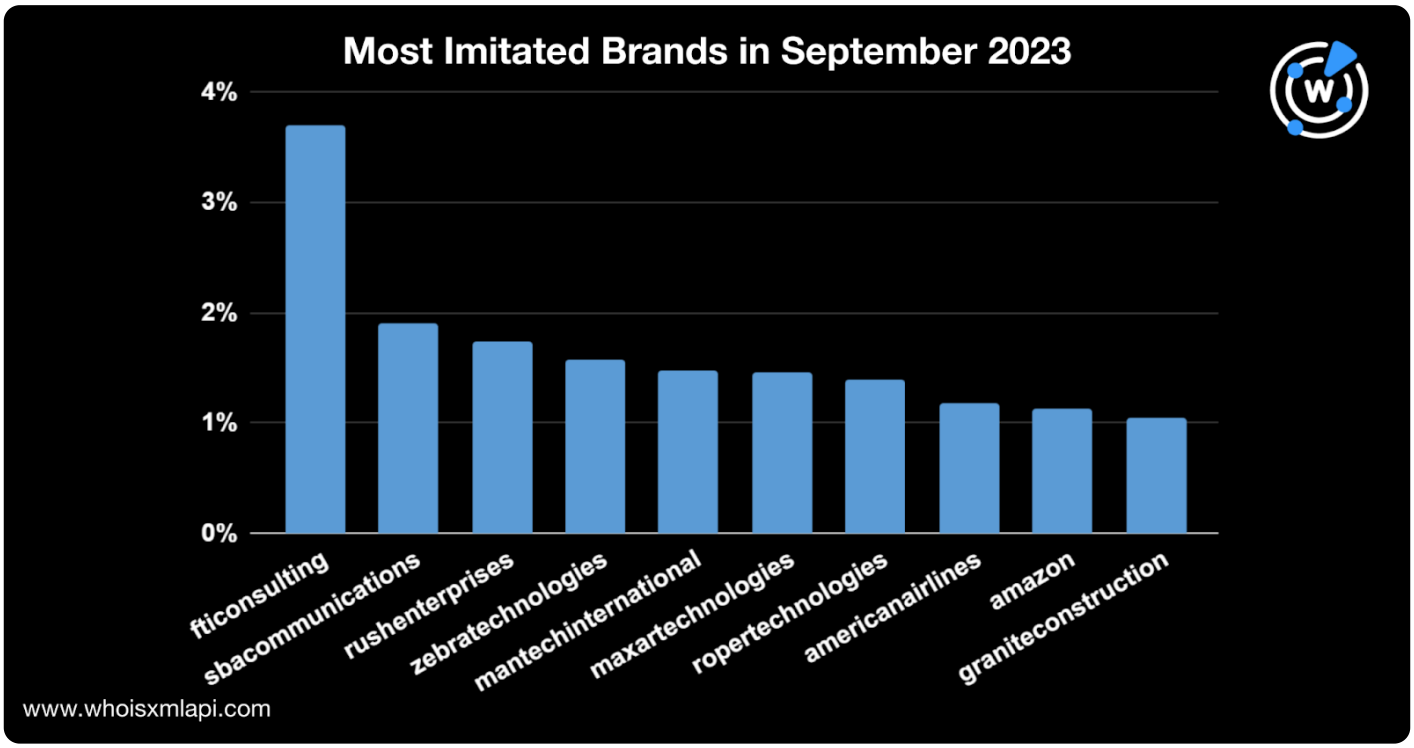
二级域名中常见的字符串

在9月份的新注册域名中，网络和科技类相关术语仍广泛使用，包括web, online, www, app,和service等。此外，market、job和home这些词也频繁出现，国际化域名持续热门，“xn”依旧流行



网络钓鱼早期预警监测

研究人员在对“网络钓鱼早期预警数据源”中数千个域名样本进行分析后，发现了一些频繁出现的术语fitco rushenterprises, zebratechnologies, nantechinternational, maxartechnologies, ropertechnologies, americanairlines, amazon, 和graniteconstruction。



从DNS角度透视本月网络安全问题

以下是我们9月份所发布的相关威胁报告。

- **Decoy Dog(诱饵狗)新型恶意软件，太过狡猾而不留DNS痕迹？** WhoisXML API
  研究人员调查了与 "诱饵狗 "相关的妥协指标 (IoC)，发现了由 90 个 IP 和 2,000
  多个字符串关联域名组成的数千个数字足迹。

- **在DNS透视下审查WoofLocker**：研究人员深入 DNS 分析了 WoofLocker
  运行八年来所报告的数百个 IoC，发现了 1,000
  多个未公布的域名，这些域名与IoC共享了专用 IP 主机和更多电子足迹。

- **通过 DNS 分析解冻 IcedID**：WhoisXML
  API研究人员发现了70多个相关联的电子足迹，包括可能与IcedID恶意软件有关联的电子邮件地址和域

- **搜索 Smishing Triad的DNS 轨迹**：我们发现了 2,500 多个可能与 Smishing Triad
  最新活动相关的域名。在这些域中，有 600 多个已被标记为恶意域名。

点击此处下载更多研究报告。

??