

2023年10月域名事件重点回顾

发布于 December 5, 2023

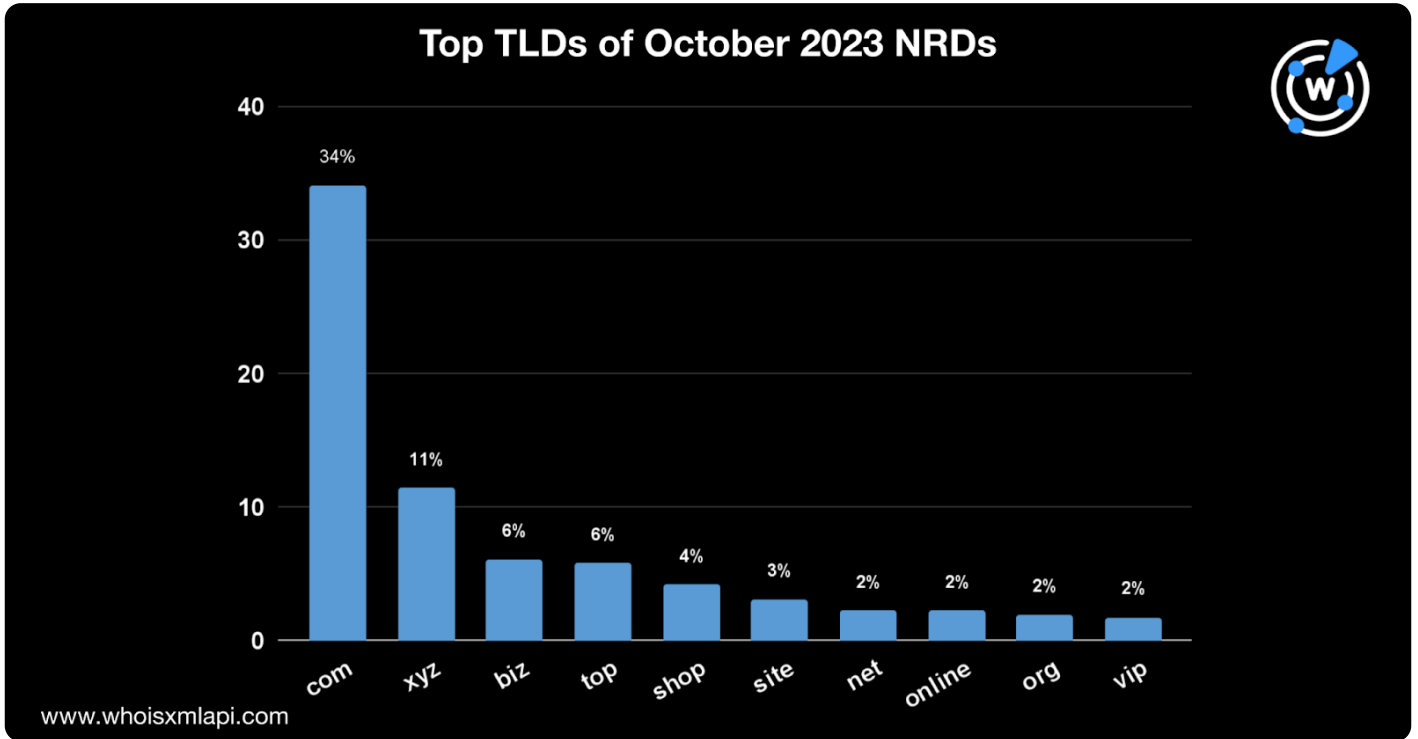
2023年10月间域名注册约数百万，WhoisXML API分析师从中随机选取了31,000个域名作为样本进行分析，研究这些域名的注册国家、注册商和顶级域情

10月新注册域名详情

顶级域分布情况

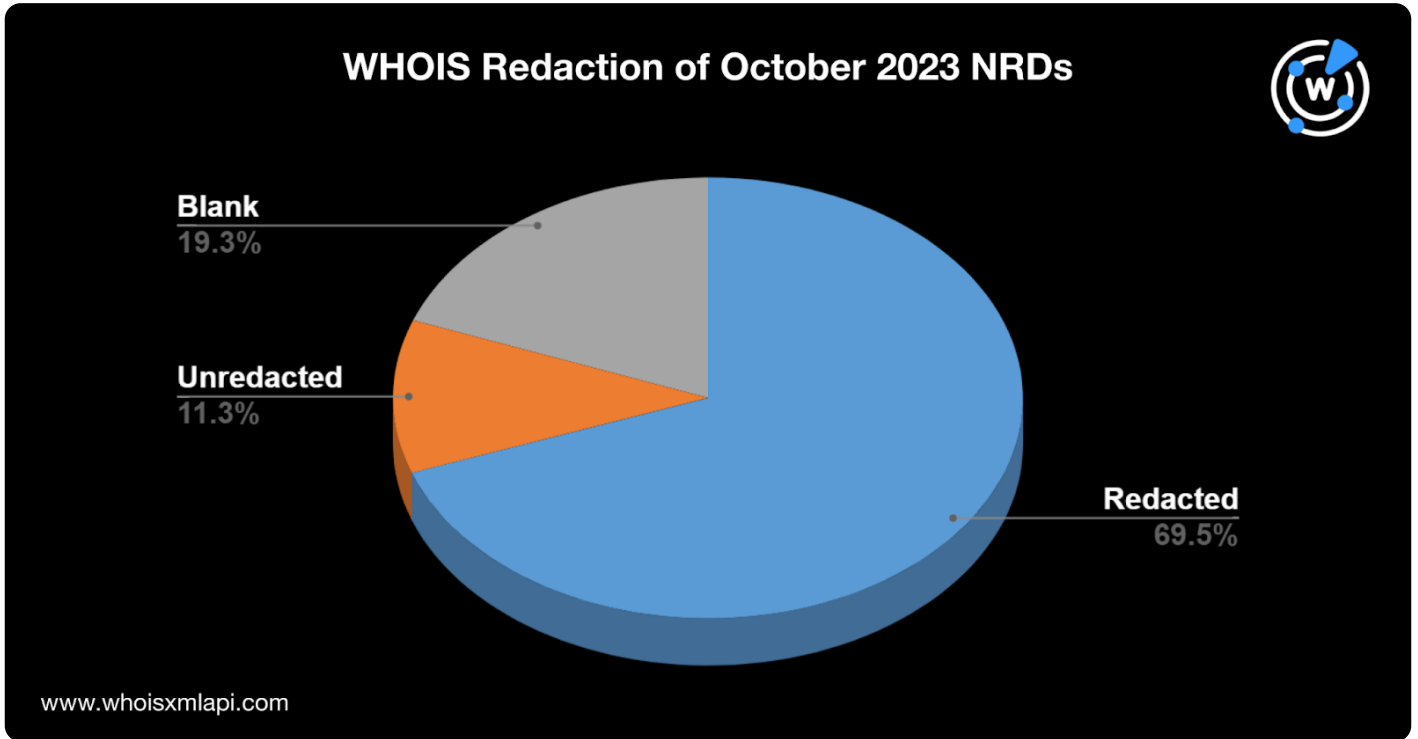
10月份中排名前十的顶级域名和前几月的情况大致相同，.com顶级域后缀仍然是使用最多的，占域名注册总量(占比11%), .biz (占比6%), .top (占比6%), .shop (占比4%), .site (占比3%), .net (占比2%), .online (占比2%), .org (占比2%), 以及 .vip (占比2%)。

排名前十的顶级域占新注册域名总量的73%，剩余27%的域名则分布在630多个顶级域中。



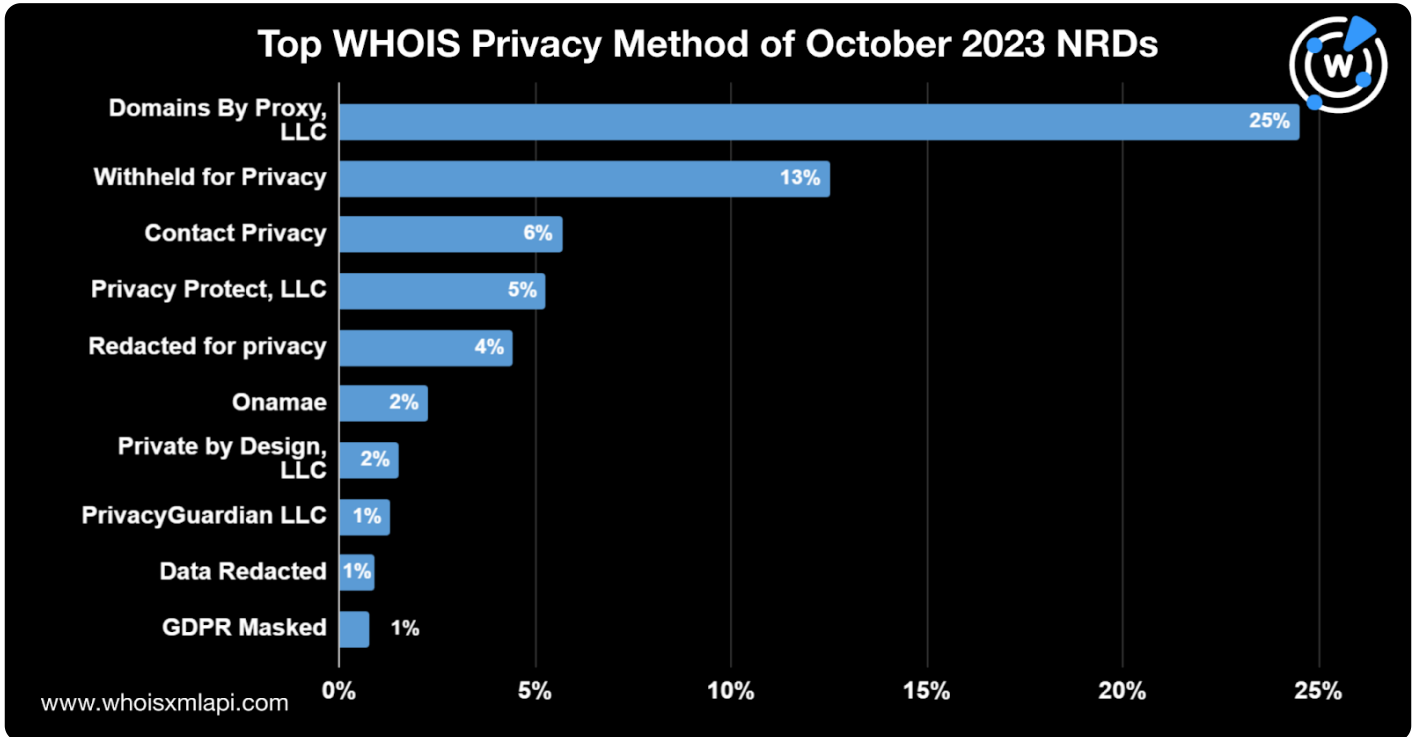
WHOIS数据编辑

约有70%的新注册域名使用了WHOIS数据编辑服务，意味着它们的注册人信息都隐藏了，只有11%的域名公



Domains By

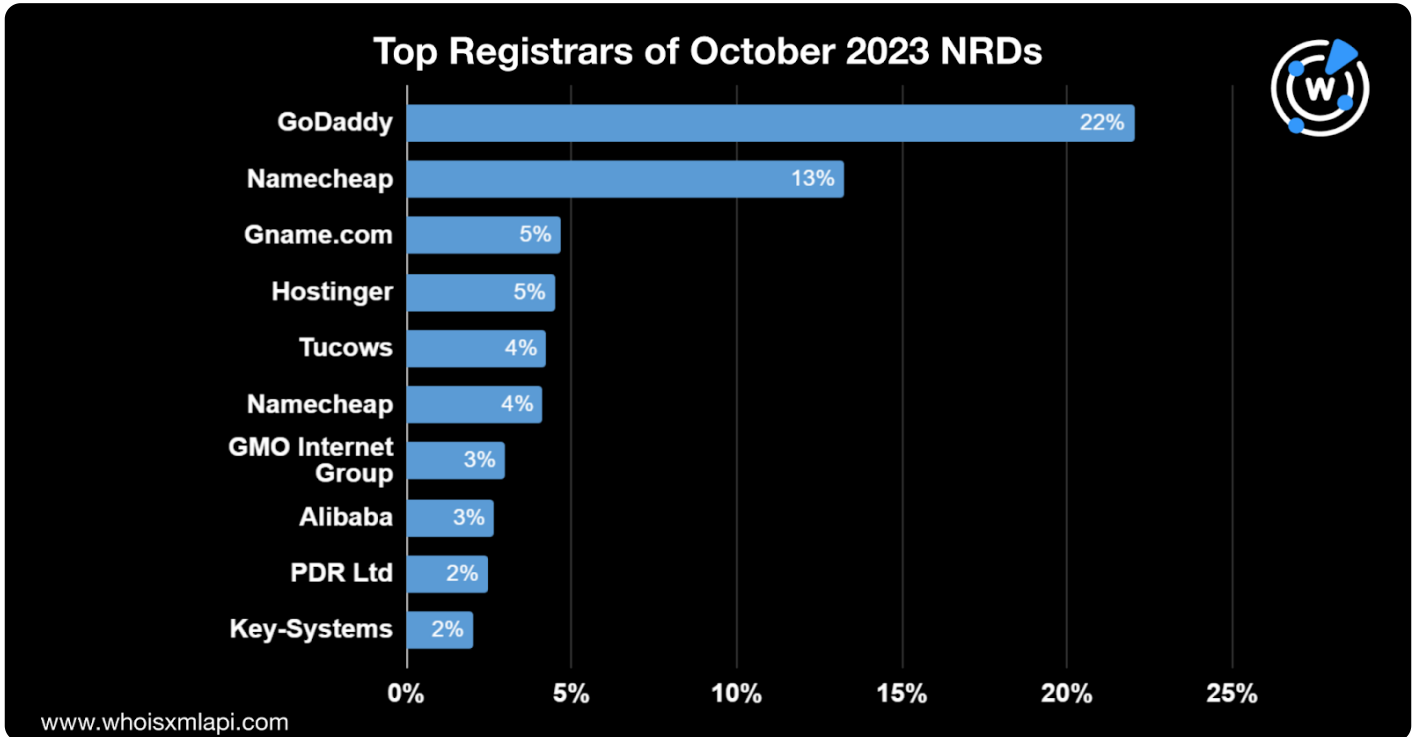
Proxy依然是最受欢迎的隐私编辑服务提供商，占新注册域名注册量的25%，紧随其后的是Withheld for Privacy，占比13%；Contact Privacy，占比6%；Privacy Protect，占比5%；Onamae和Private by Design 分别占比2%；以及Privacy Guardian占比1%。



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

注册商分布

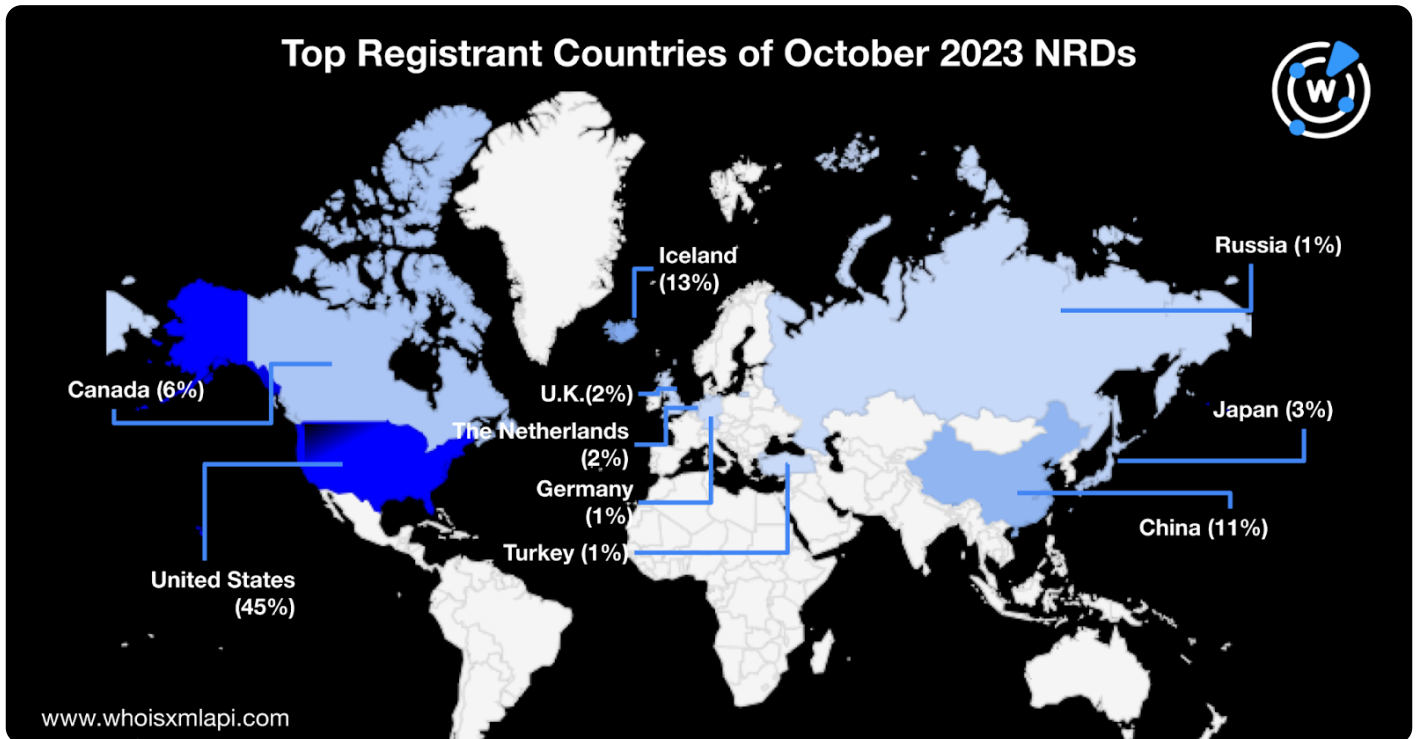
10月份注册商排名中，GoDaddy依旧领先，占新域名注册总量的22%。Namecheap排名第二，占比约为13%。Internet Group和Alibaba，分别占比3%，以及PDR Ltd.和Key-Systems，分别占比2%。



排名前十的注册商占据了域名注册总量的63%，剩余37%的域名则分布在350多家其他的注册商中。

排名领先的注册国家

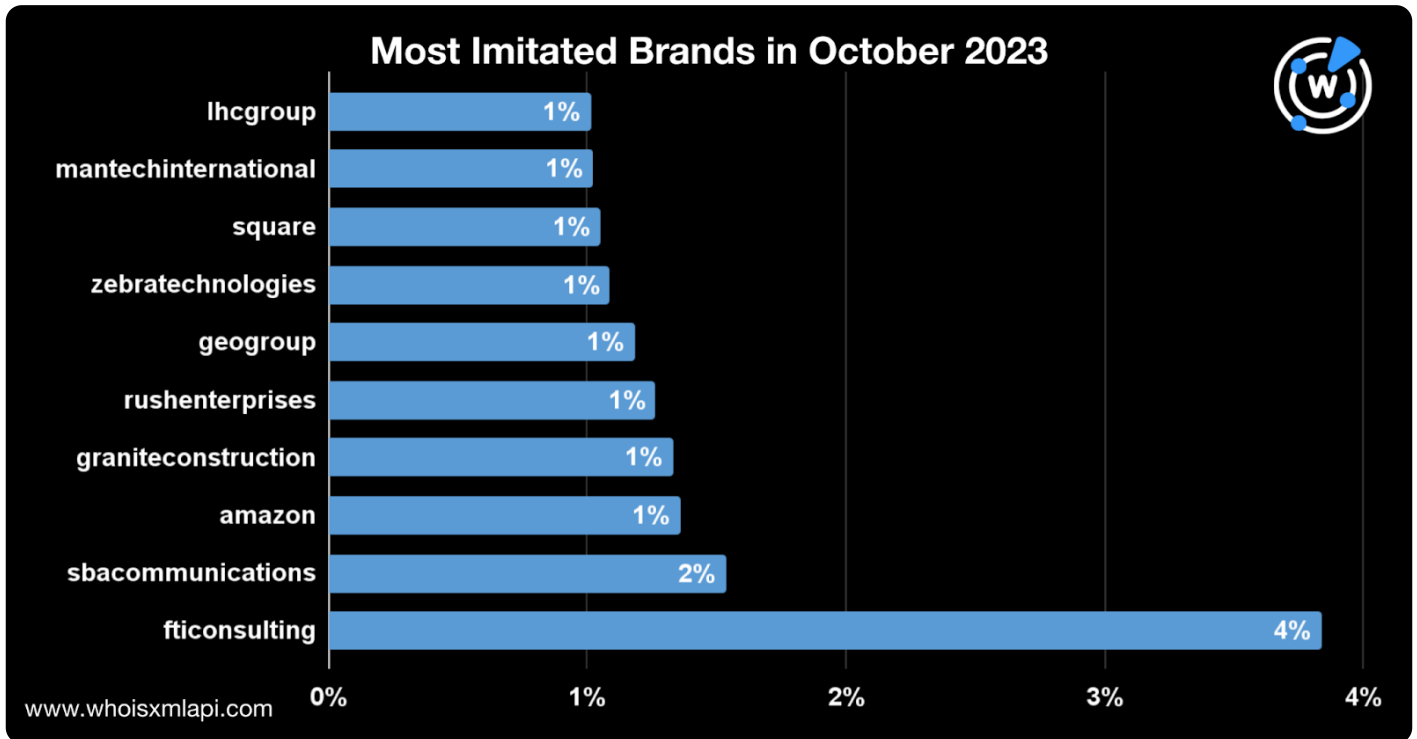
在10月份的新域名注册中，美国依旧是排名领先的国家（占比45%），冰岛和中国紧随其后，分别占13%和11%。剩余排名前十的注册国家依次为加拿大（6%）、日本（3%）、英国（2%）、荷兰（2%）、俄罗斯



排名前十的注册国家占域名注册总量的85%，剩下15%的域名则分布在130多个其他国家中。

二级域名中常见的字符串

在10月份的新注册域名中，互联网相关术语仍广泛使用，包括service, online, test, 和shop等。此外，go, hit, job, market, gem, 和game这些词也频繁出现。国际化域名持续热门，“xn”依旧流行使用。



从DNS角度透视本月网络安全问题

以下是我们10月份所发布的相关威胁报告。

- **网络钓鱼机构滥用.top域名**：WhoisXML API威胁分析员Dancho Danchev发现了一个滥用.top域名从事网络钓鱼的行动，从而指引了研究团队发现了4,000多个额外相关链接。
- **在DNS中寻找二维码网络钓鱼痕迹**：在WHOIS和DNS情报的帮助下，WhoisXML API研究人员将标记为与二维码钓鱼代码活动相关的妥协指标 (IoC) 的 18 个 URL 进行了扩展搜索，发现了 10,000 多个相关联的域名。
- **使用DNS网络捕捉Messenger钓鱼足迹**：最近WhoisXML API团队调查了MrTonyScam，这是一个针对Facebook企业账户的恶意软件，从事网络钓鱼活动以感染受害者使用设备的形式窃取其密码。通过攻击者所留痕迹，我们发现了十几个公共电子邮件地址和 1,000 多个与威胁 IoC 共享相同电子邮件地址和字符串的域名。

您可[点击此处](#)查找更多报告内容。

??