2023年8月域名事件重点回顾

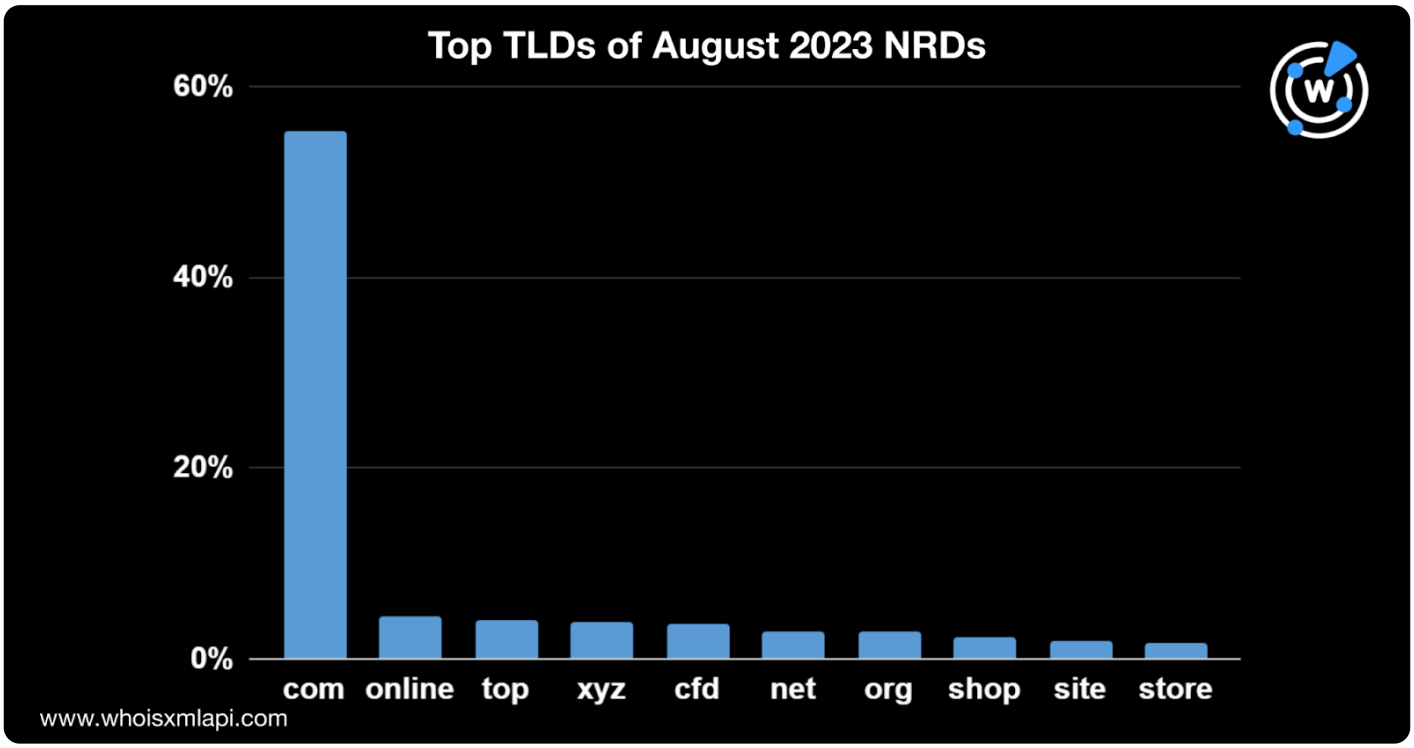
发布于 November 1, 2023

2023年8月1日-31日期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

8月新注册域名详情

顶级域分布情况

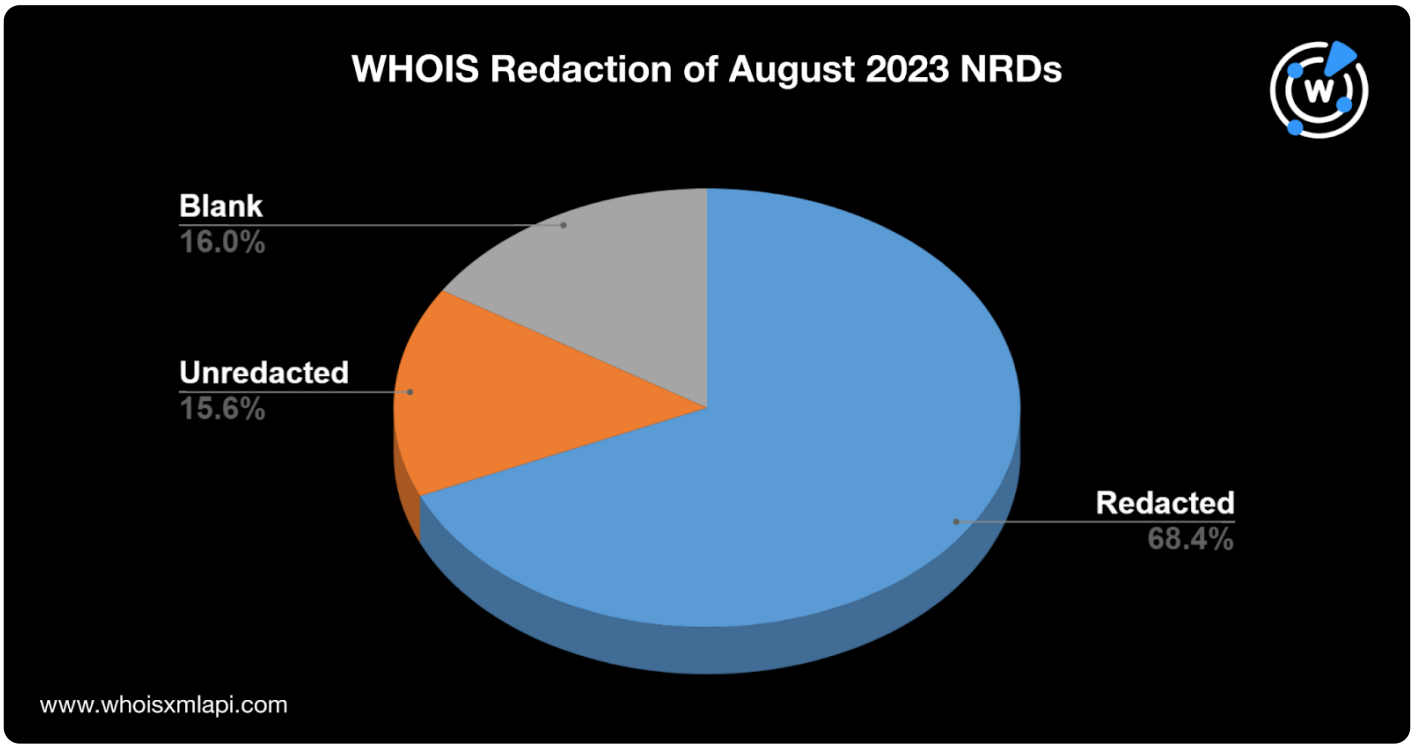
8月份中排名前十的顶级域名和前几月的情况保持基本一直，.com顶级域后缀仍然是使用最多的，占域名注
和 .cfd 分别为4%；.net 和 .org 分别为3%；.shop、.site 和 .store分别为 2%。



排名前十的顶级域占新注册域名总量的83%，剩余17%的域名则分布在620多个顶级域中。

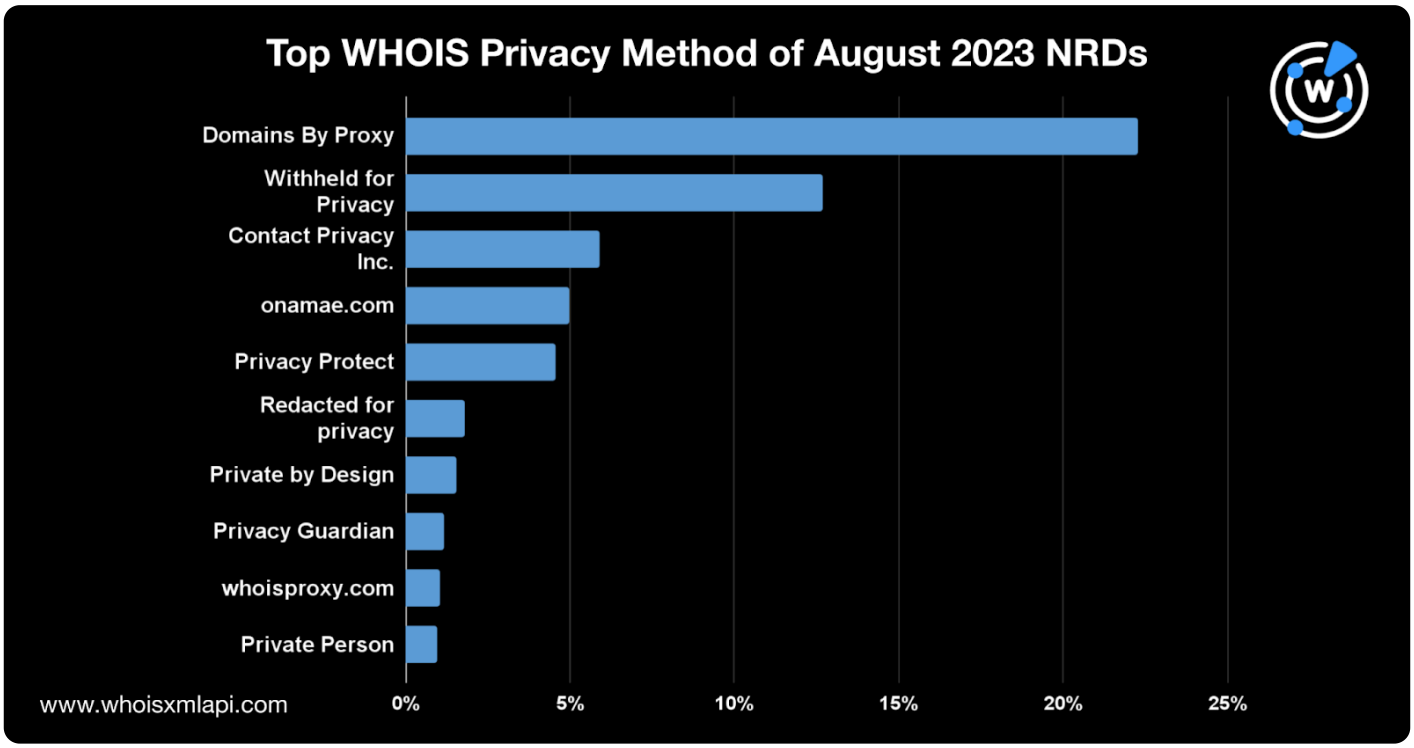
WHOIS 数据编辑

大多数新注册域名使用了WHOIS数据编辑服务，只有15.6%的域名则公开其注册机构，而约16%的域名则在



Domains By

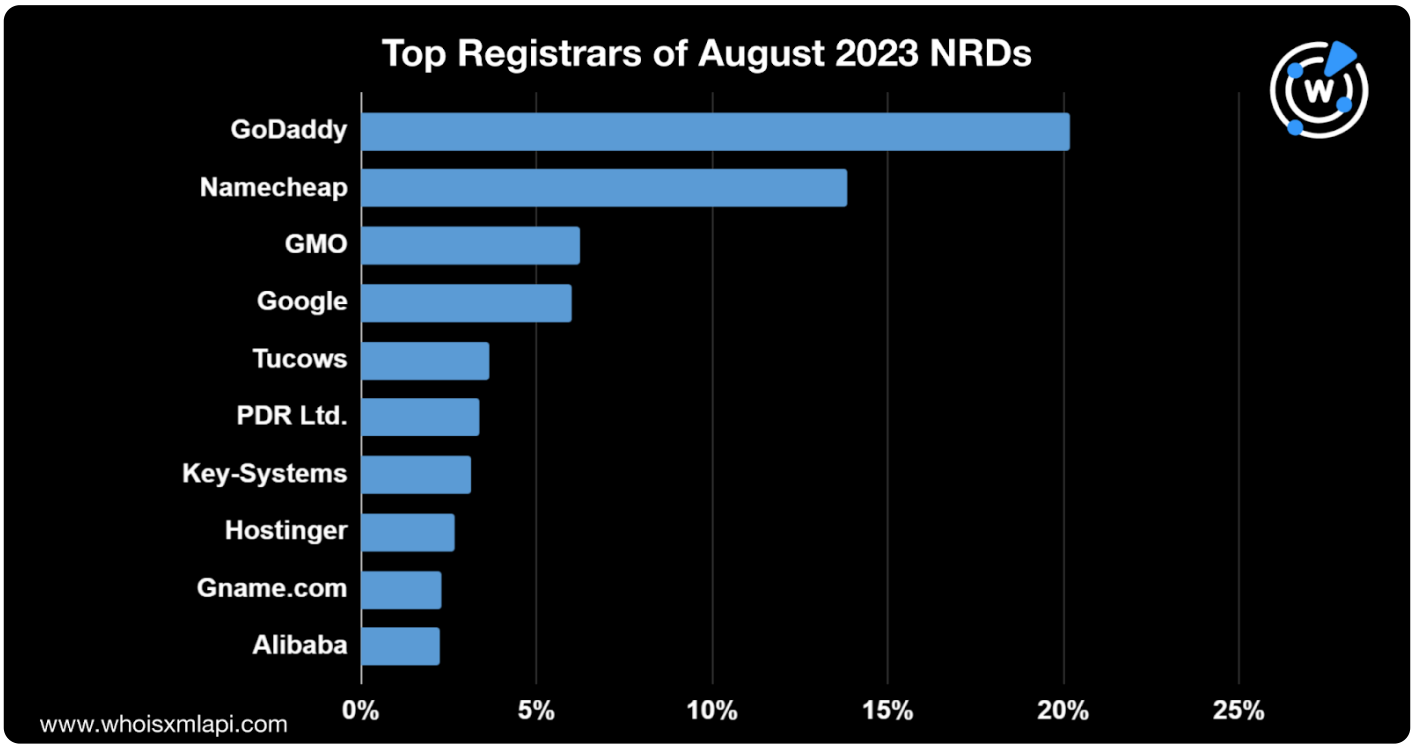
Proxy依然是最受欢迎的隐私编辑服务提供商，占比新注册域名注册量的22%，紧随其后的是Withheld for Privacy，占比13%；Contact Privacy，占比为6%; Onamae，占比为5%；Privacy Protect, LLC，占比为5%; Private by Design为2%；PrivacyGuardian.org和Whoisproxy分别为1%。



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

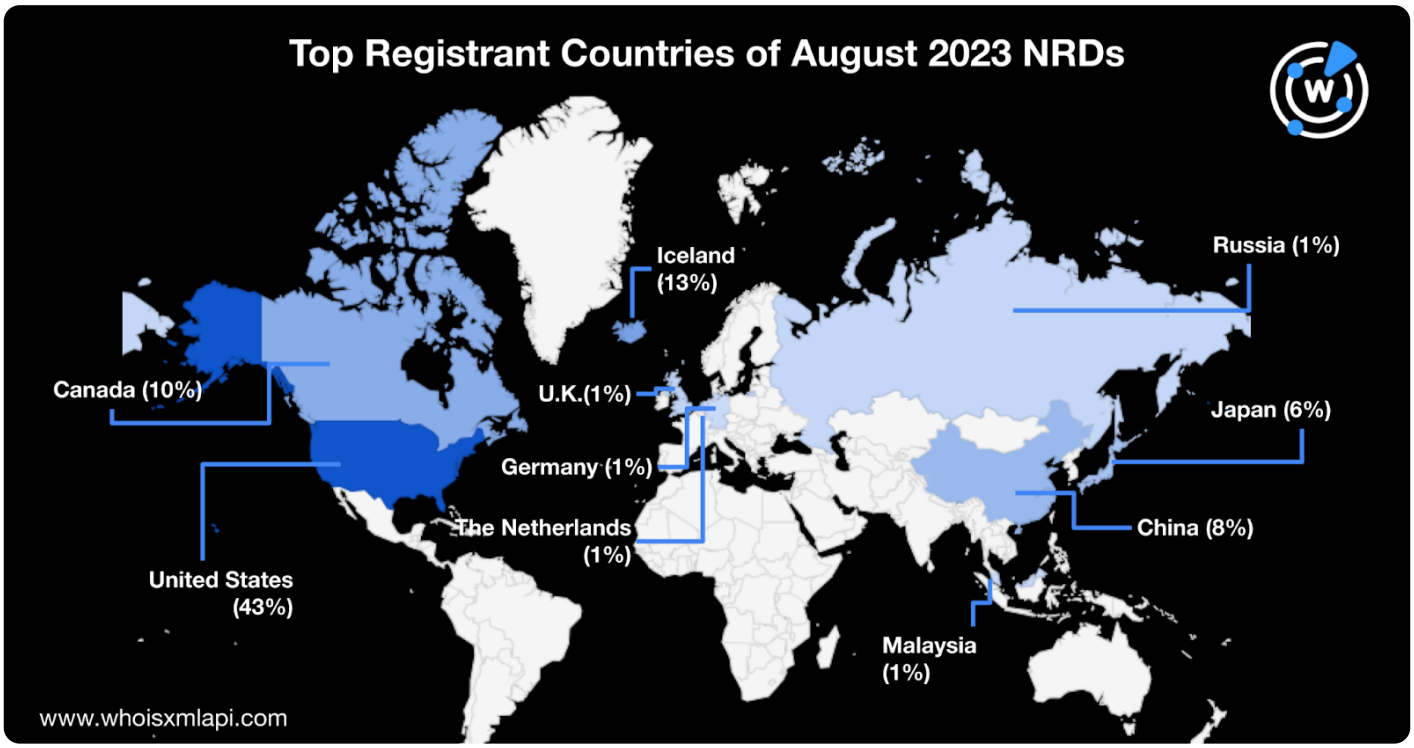
8月份的注册商排名中，GoDaddy独占鳌头，占域名注册总量的20%。Namecheap排名第二，占比约为14%(占比6%)和GMO Internet (占比6%), Tucows (占比4%), Key-Systems和Hostinger（分别为3%），Gname.com和Alibaba（分别为2%）。



排名前十的注册商占据了域名注册总量的64%，剩余的域名则分布在400多家其他的注册商中。

排名领先的注册国家

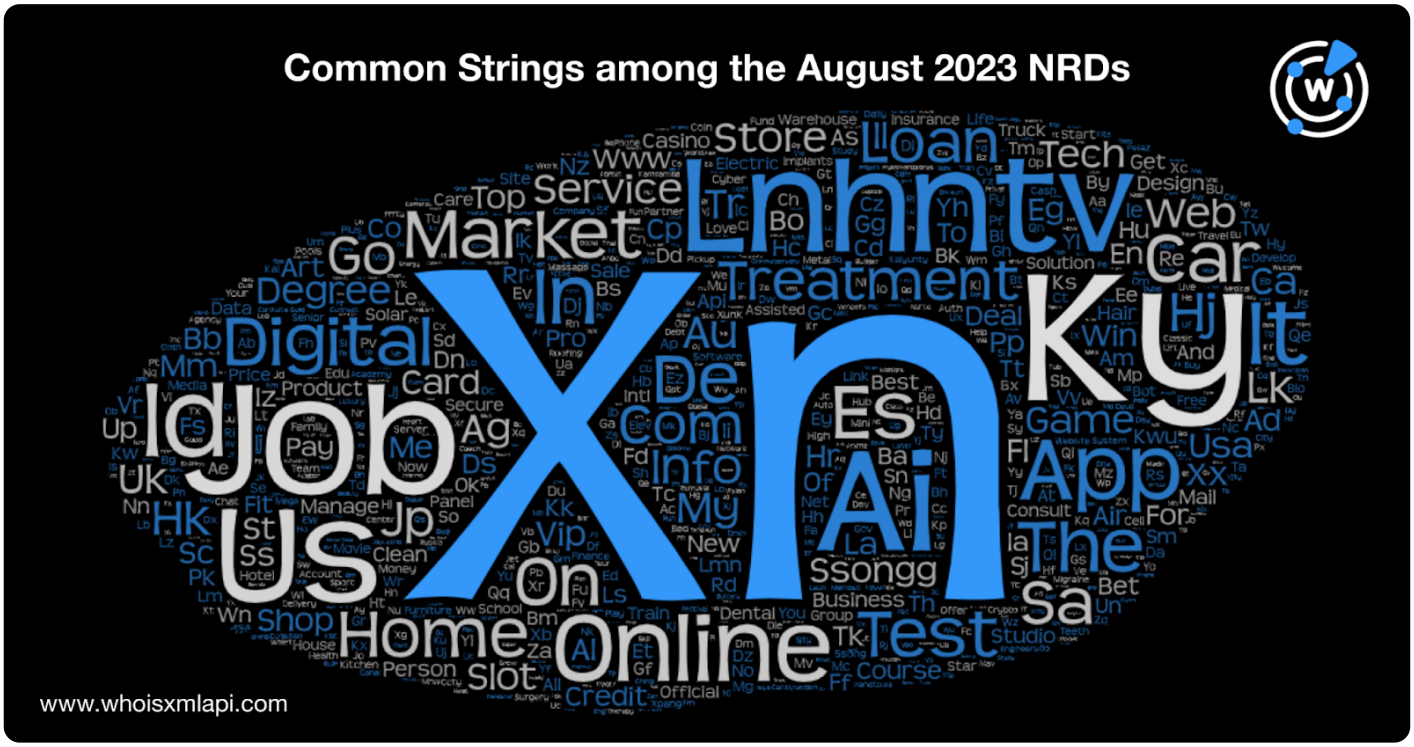
在8月份的新域名注册中，美国依旧是排名领先的国家（占比43%），冰岛和加拿大紧随其后，分别占13% 和
10%。剩余排名前十的注册国家依次为中国（8%）、日本（6%）、英国（2%）、俄罗斯（1%）、马来西



排名前十的注册国家占域名注册总量的87%，剩下的域名则分布在130多个其他国家中。

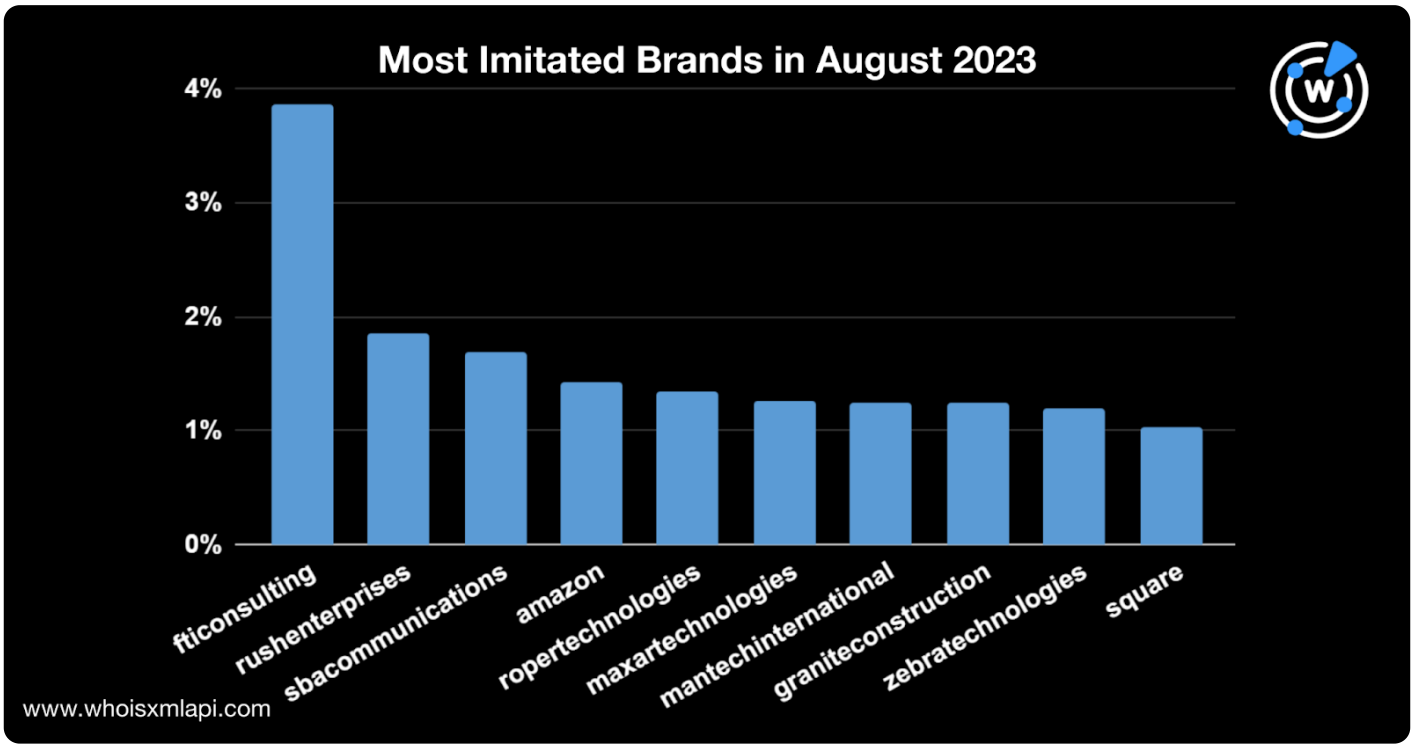
二级域名中常见的字符串

在8月份的新注册域名中，网络和科技类的术语仍广泛使用，如app, online, service,和digital等。此外，loan, job, 和home这些词也频繁出现，国际化域名持续热门，“xn”依旧流行使用。



网络钓鱼预警监测

研究人员从“网络钓鱼预警数据源”中分析了数千个域名样本，确定了一些被模仿频次最多的品牌。在数据
ropertechnologies, maxartechnologies, mantechinternational, graniteconstruction, zebratechnologies, 和square这些字符各占网络钓鱼预警域名数量的1%。



从DNS角度透视本月网络安全问题

以下是我们8月份所发布的相关威胁报告。

- **Redis是否还会继续成为威胁者的雷达？** WhoisXML API 研究人员调查了与 CVE-2022-0543 或 Redis Lua 沙箱逃逸和远程代码执行漏洞相关的妥协指标 (IoC)，发现了 20,000 多个包含 redis 字符串的网络域名。

- **在 DNS 中查询 WyrmSpy 和 DragonEgg 与 APT41 的关联性：** WhoisXML API 试图通过查验公开的妥协指标（IoCs） 来确定 APT41 与 WyrmSpy 和 DragonEgg 之间的联系。

- **JumpCloud 供应链攻击背后的 DNS 透视：** 我们的研究人员对 JumpCloud 供应链攻击的 IoC 进行了DNS方面的深入研究，发现了数百个潜在的相关联的域名。

- **人工智能工具的流行：是否会成为发起恶意活动的机遇？** WhoisXML API 和 Bayse Intelligence 联手进行了相关研究，发现并确认了2023年八款可用于攻击行为的最佳人工智能工具的网络域名属性

点击此处下载更多研究报告。

??