

2023年7月域名事件重点回顾

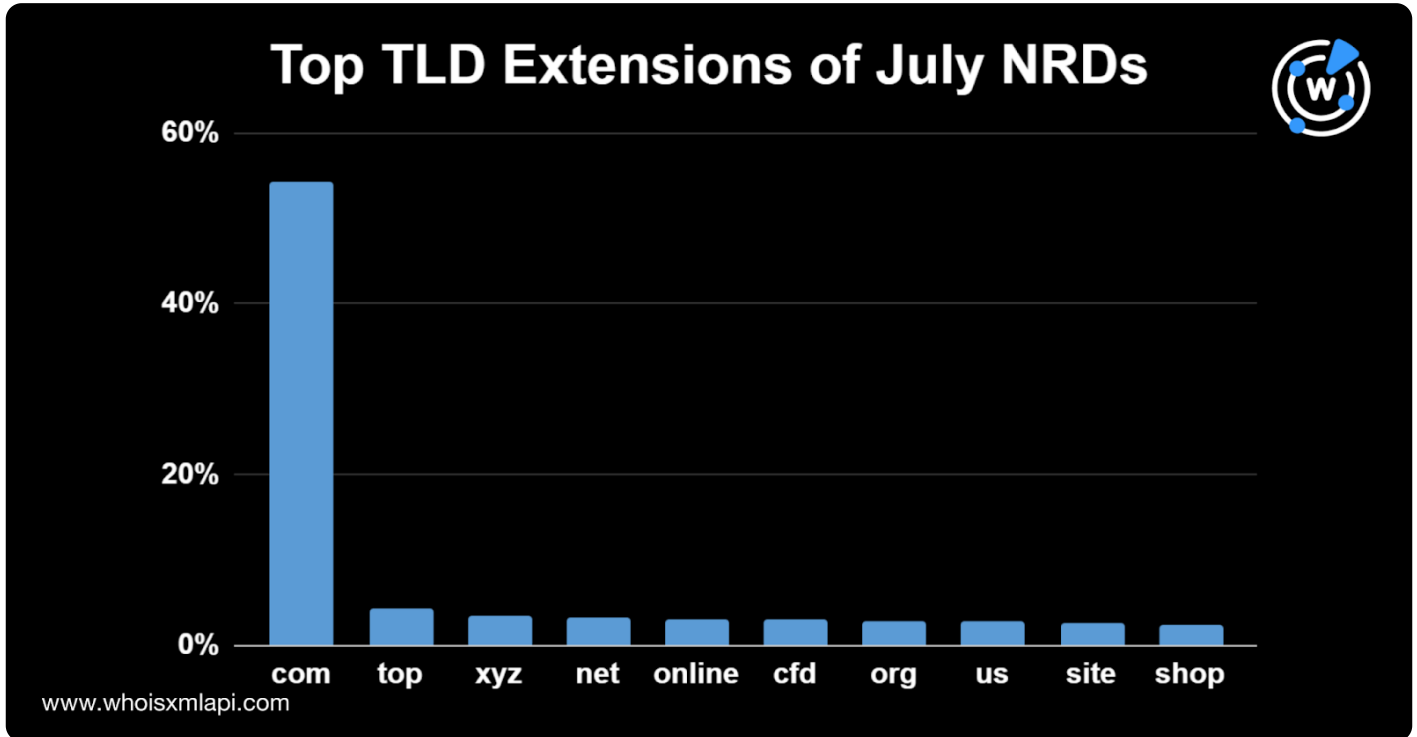
发布于 August 25, 2023

2023年7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

7月新注册域名详情

顶级域分布情况

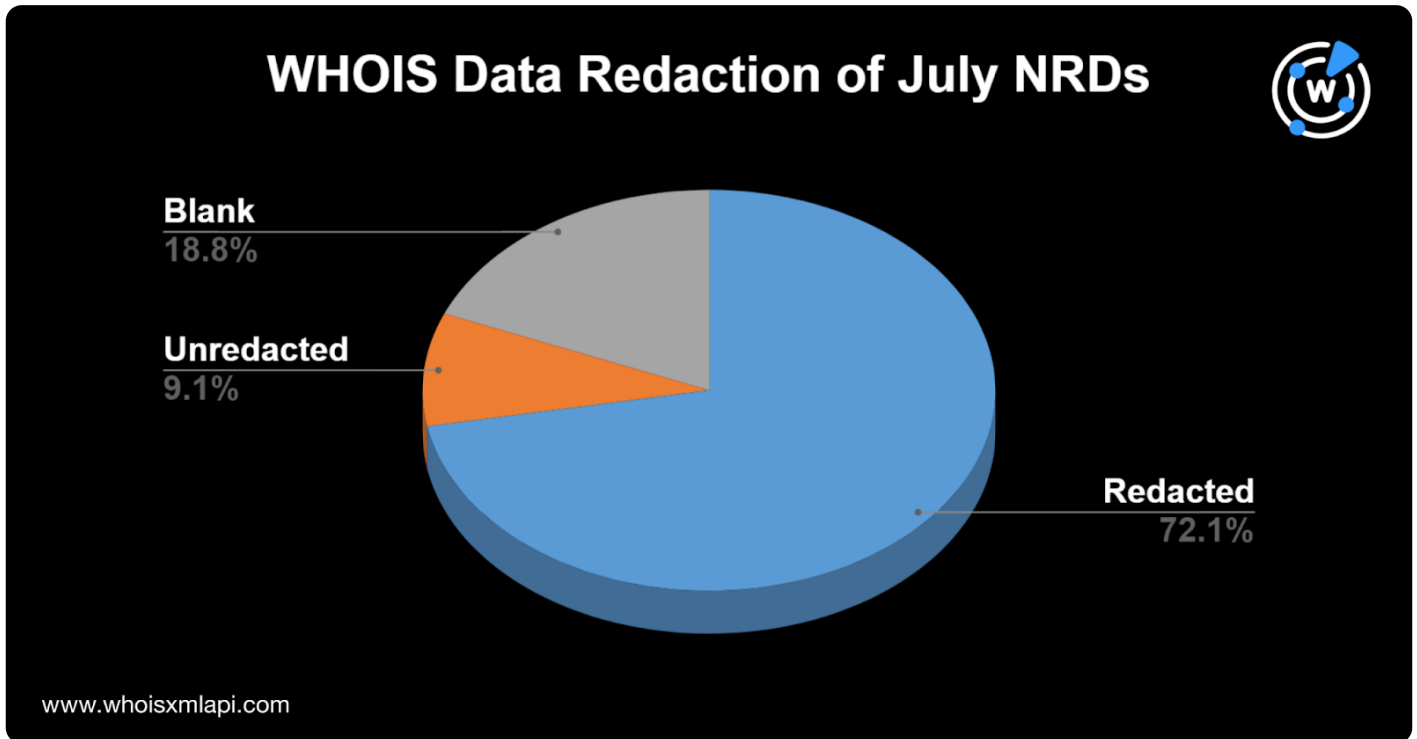
除了.info被.us代替以外，6月份中排名前十的其他顶级域名在7月份的表现依旧势头强劲，.com顶级域后缀(4%)，.xyz (3%)，.net (3%)，.online (3%)，.cf (3%)，.org (3%)，.us (3%)，.site (3%)以及.shop (2%)。



排名前十的顶级域占新注册域名总量的82%，剩余18%的域名则分布在620多个顶级域中。

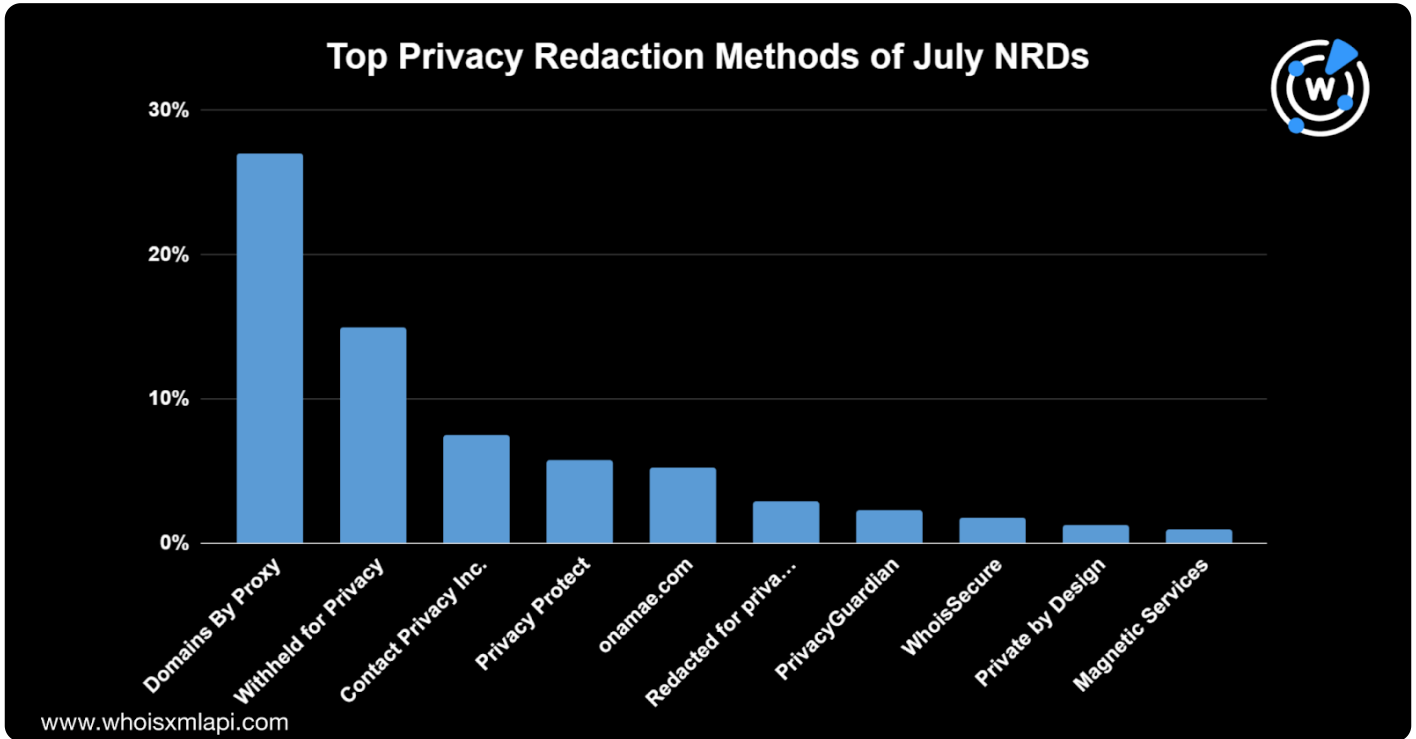
WHOIS 数据编辑

大多数新注册域名使用了WHOIS数据编辑服务，只有9%的域名则公开其注册机构，而约19%的域名则在此



Domains By

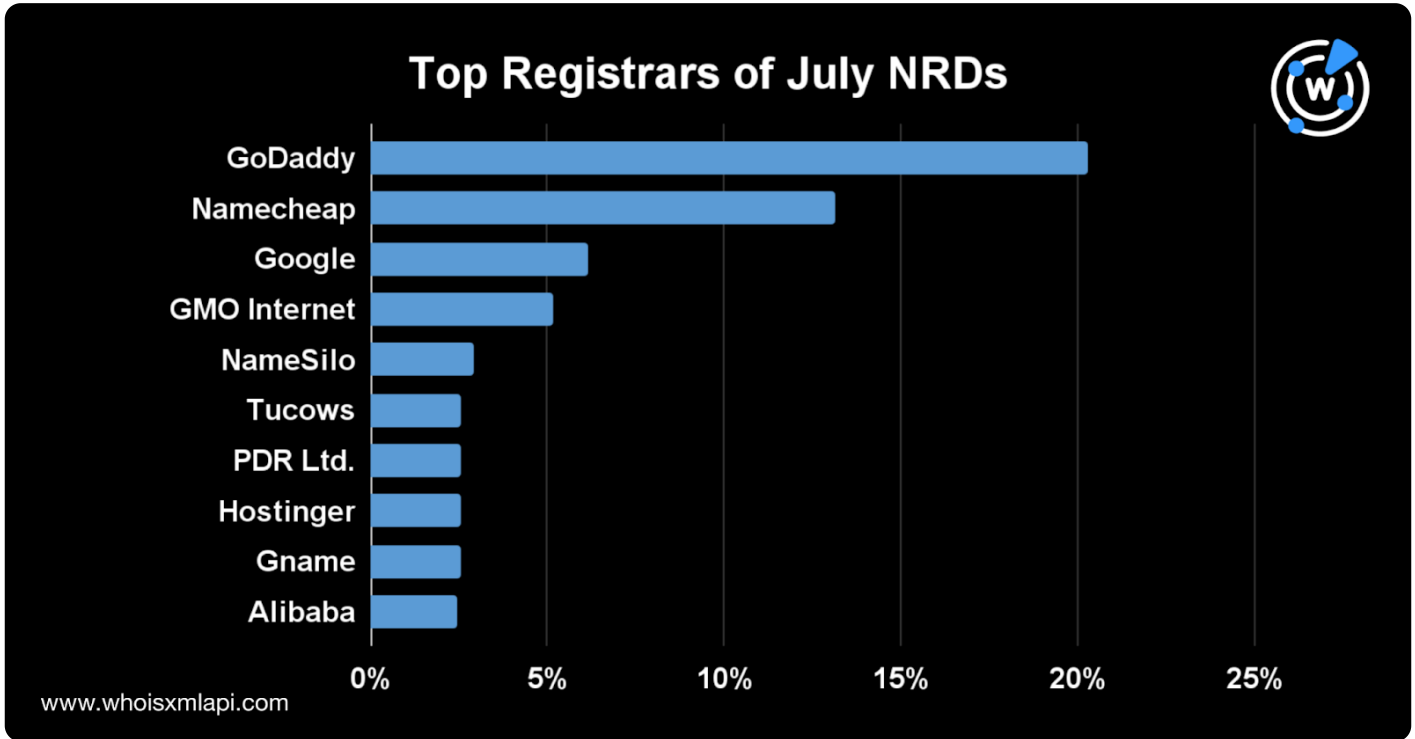
Proxy依然是最受欢迎的隐私编辑服务提供商，占比新注册域名注册量的27%，紧随其后的是Withheld for Privacy，占比15%；Contact Privacy，占比为7%；Privacy Protect, LLC，占比为6%；Onamae 5%；PrivacyGuardian.org和WhoisSecure 分别为2%；以及Private by Design和Magnetic Services分别为1%。



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

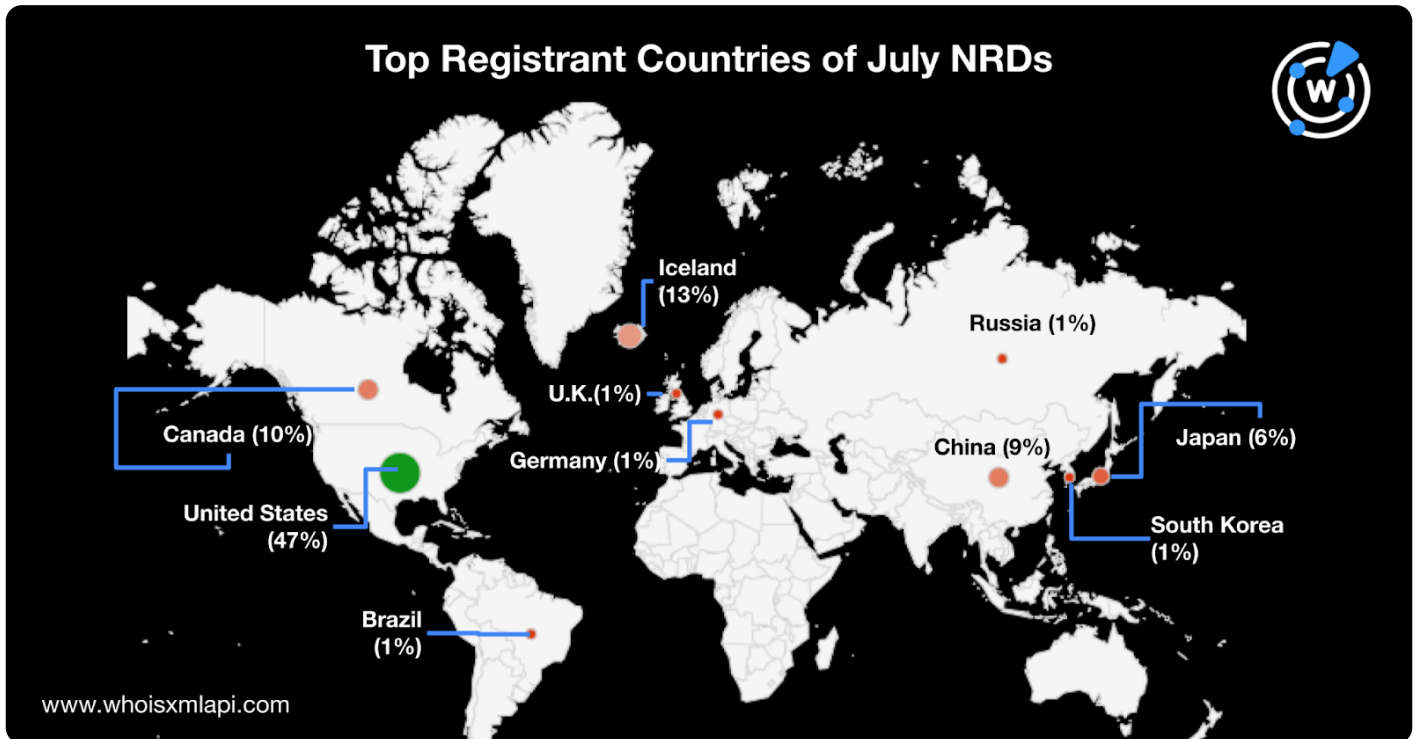
7月份的注册商排名与6月份保持一直，GoDaddy独占鳌头，占域名注册总量的20%。Namecheap位居第二(占比7%), GMO Internet (占比6%), Hostinger和Tucows (分别为4%), Alibaba和Gname.com (分别为3%), 以及PDR Ltd. 和NameSilo (分别为2%)。



排名前十的注册商占据了域名注册总量的60%，剩余的域名则分布在430多家其他的注册商中。

排名领先的注册国家

7月份中接近一半儿的新域名是在美国注册的（占比47%），同前几月类似，冰岛和加拿大紧随其后，分布

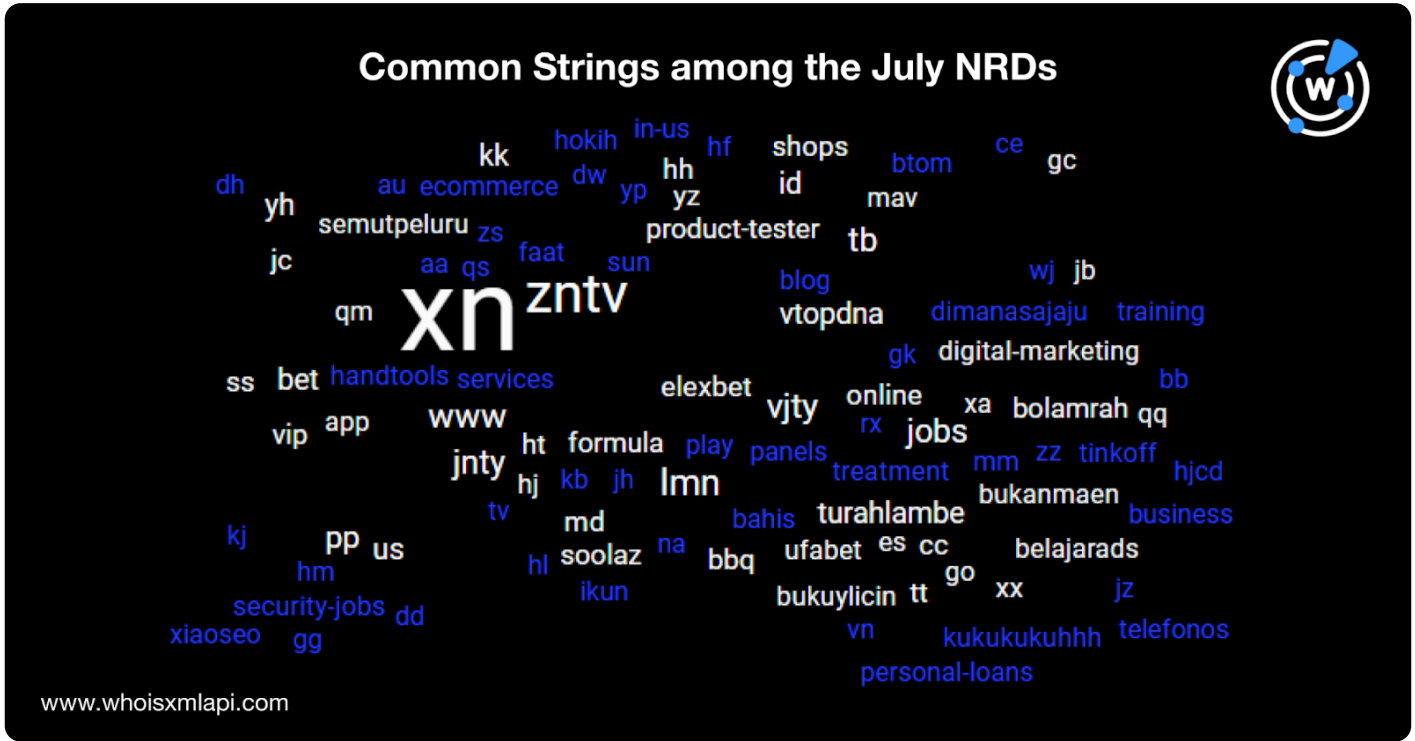


排名前十的注册国家占域名注册总量的89%，剩下的域名则分布在130多个其他国家中。

二级域名中常见的字符串

在新域名中，网络和科技类的术语会被广泛使用，如app, digital-marketing, e-commerce, services, security-jobs, 和shops等。

此外，“bet”一次也频繁出现，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7月份所发布的相关威胁报告。

- **DNS深度挖掘恶意软件加密**：WhoisXML API研究人员通过对恶意软件加密服务相关的妥协指标列表进行分析，发现了上百个域名托管在了由攻
- **黑客BlackCat再次攻击Reddit，通过DNS揭秘其踪迹**：我们的研究人员分析了与近期网络攻击Reddit相关的十多个已被标记为妥协指标的IP地址，结果导向
- **通过DNS情报识别MOVEit Exploit-CLOP勒索软件威胁载体**：我们的研究人员调查了与MOVEit-enabled CLOP勒索软件攻击相关的139个IoC，发现了6600多个域名包含有字符串zoom。

??