2023年12月域名事件重点回顾

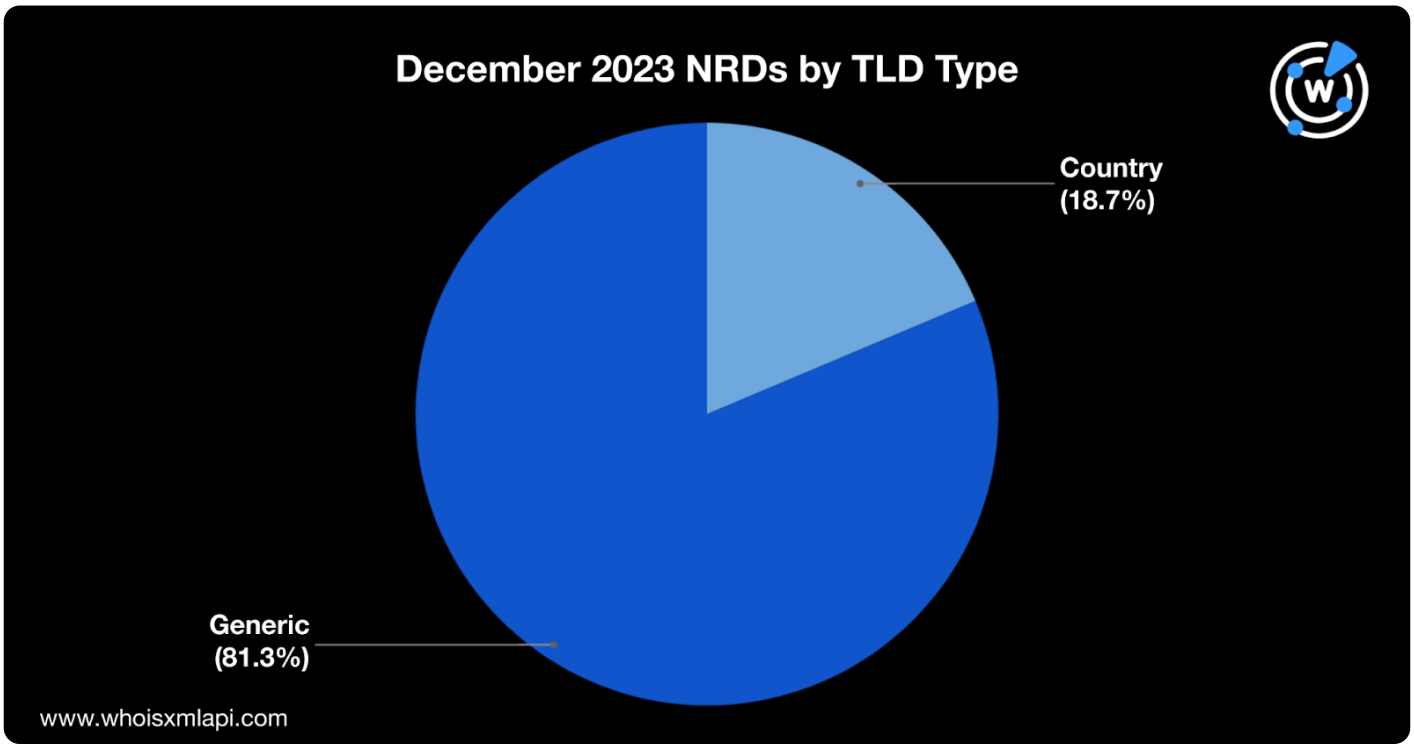
发布于 February 2, 2024

WhoisXML
API分析师选取了2023年12月1日至31日期间注册的960万个域名作为样本进行分析，研究这些域名的发展趋

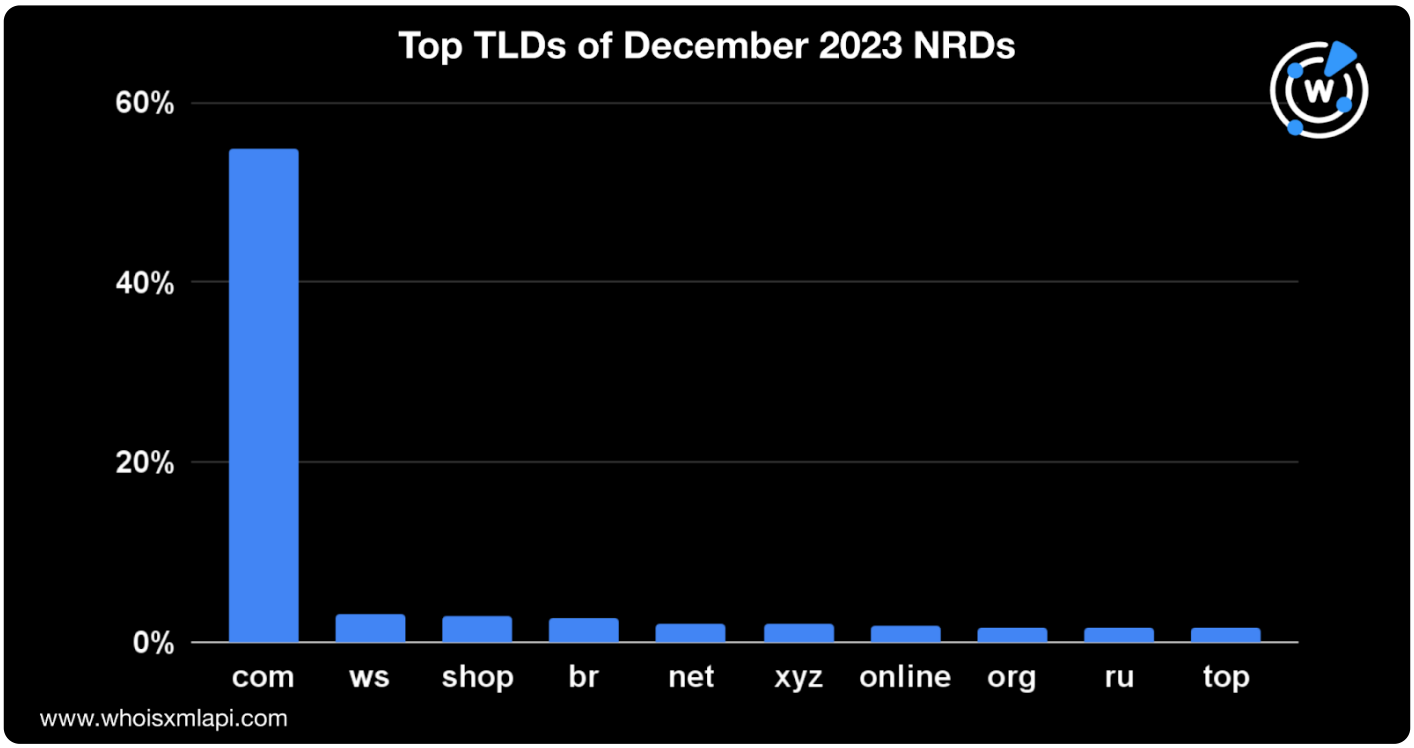
12月新注册域名详情

顶级域分布情况

通用顶级域（gTLD）占新注册域名总数的 81.3%，国家代码顶级域（ccTLD）则占比 18.7%。

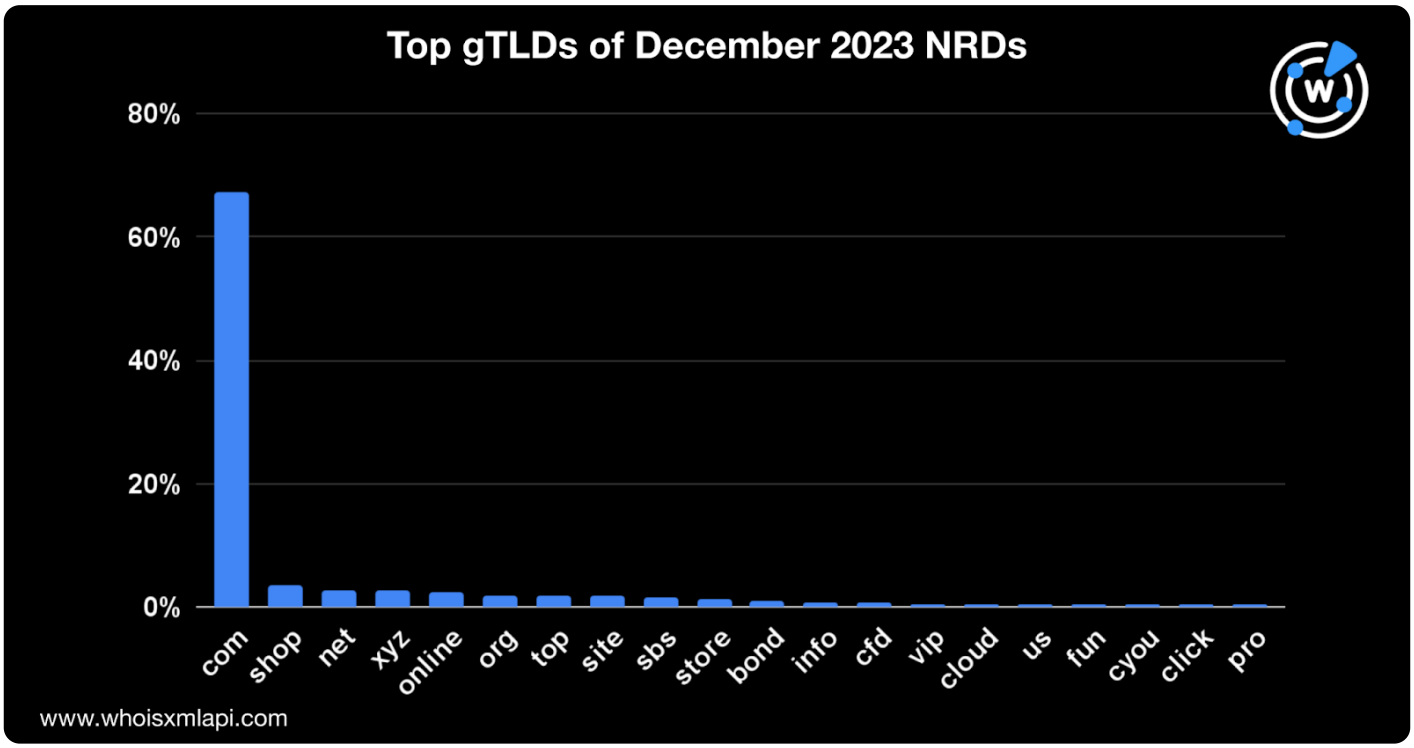


总体来说，.com顶级域后缀占新域名注册总量的54.8%，紧随其后的是.ws（占比3.1%），.shop（占比3%
.org（占比1.6%）和.ru及.top（分别占比1.5%）。

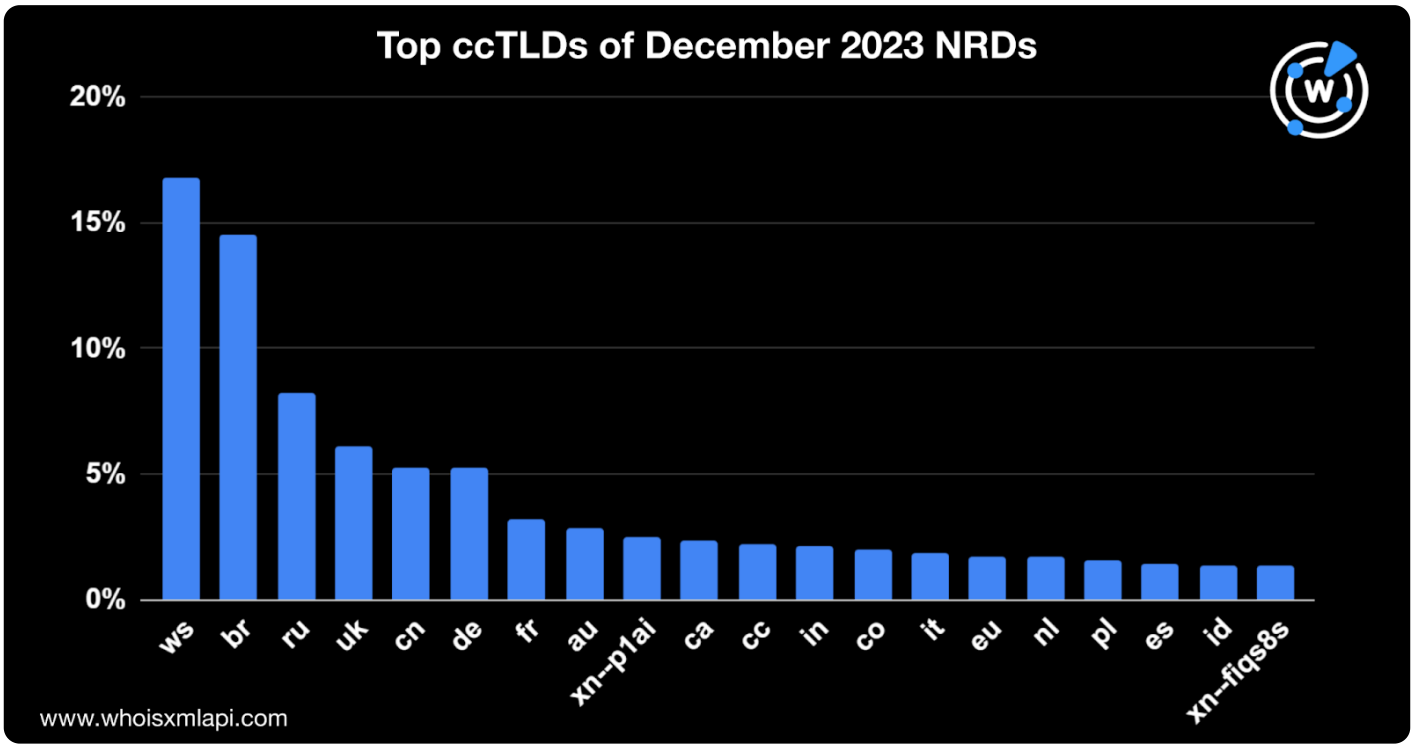


随后，我们对每一种顶级域的使用情况进行了单独分析，确定了最常用的通用顶级域和国家代码顶级域。

在超过625个通用顶级域中，.com是使用最多的通用顶级域后缀，占所有通用顶级域的新注册域名总数的6
和 .xyz(分别占 2.6%)、.online(2.4%)、.org 和 .top (分别占 1.9%)、.site (1.8%)、.sbs
(1.6%)、.store 和 .bond (分别占 1.2%)、.info (0.9%)、.cfd (0.7%)、.vip、.cloud、.us 和 .fun
(分别占 0.5%)，以及 .cyou、.click 和 .pro (分别占 0.4%)。

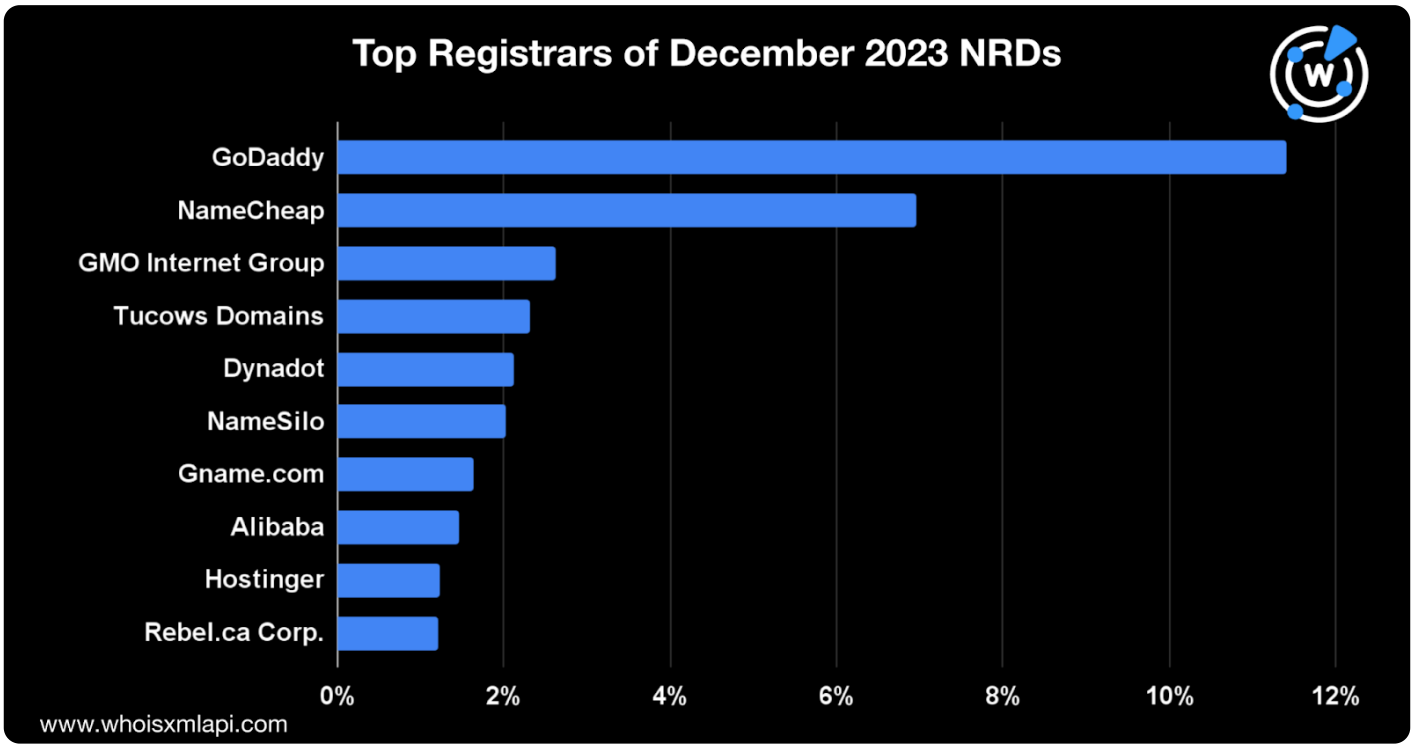


同时，在 240 多个国家顶级域名中，.ws 最受欢迎，占 12 月份新注册域名量的16.8%。其次是.br（占比14.6%）、.ru（占比 8.3%）、.uk（6.1%）、.cn和.de（各占比5.2%）、.fr（3.2%）、.au（2.8%）、.xn--p1ai（2.5%）、.ca（2.4%）和.cc（2.2%）。排名前 20 的其他国家顶级域名如下图所示。



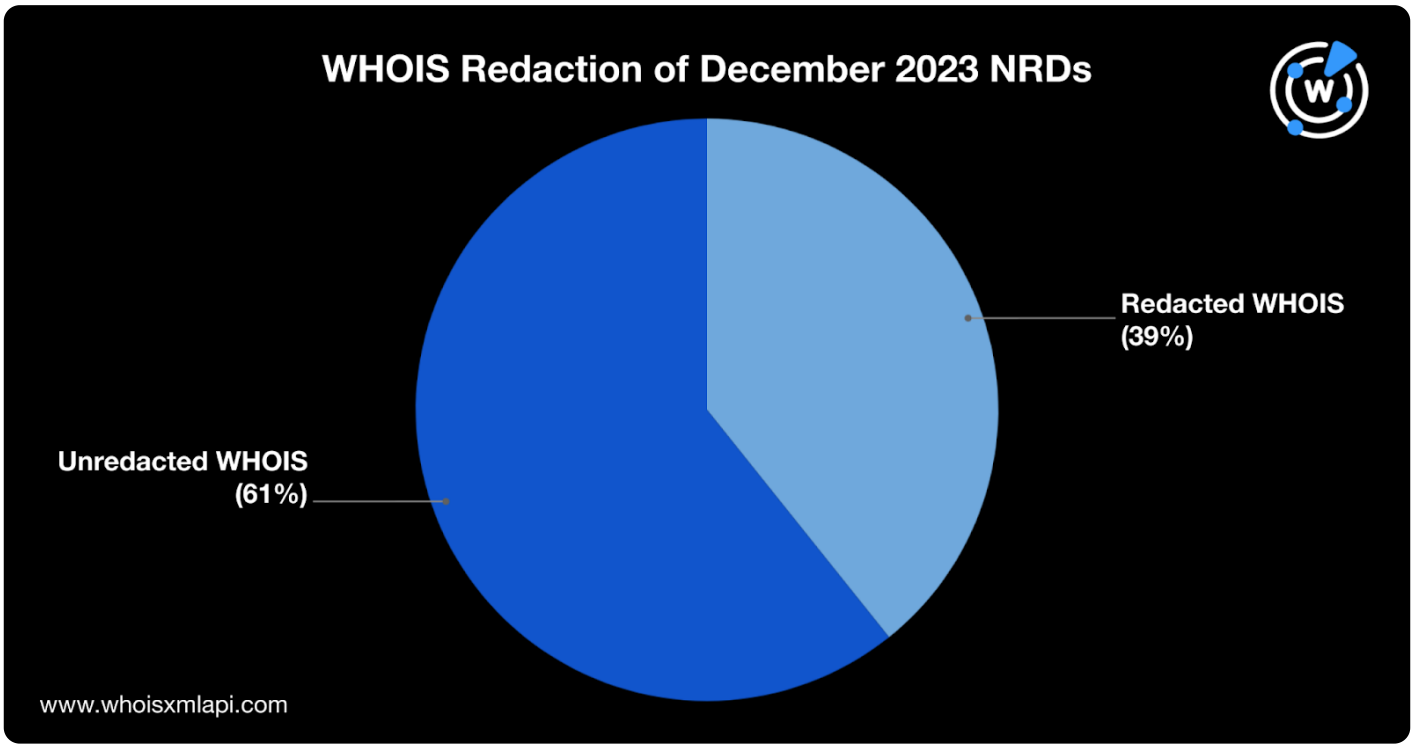
注册商分布

GoDaddy
依然是12月份排名领先的注册商，占据了新注册域名总量的11.4%。Namecheap公司以7%的份额紧随其后Internet 占比2.6%，Tucows 占比2.3%，Dynadot占比2.1%，NameSilo占比2%，Gname占比1.6%，阿里巴巴云计算公司占比1.5%，Hostinger 和 Rebel.ca 各占比1.2%。



WHOIS数据编辑

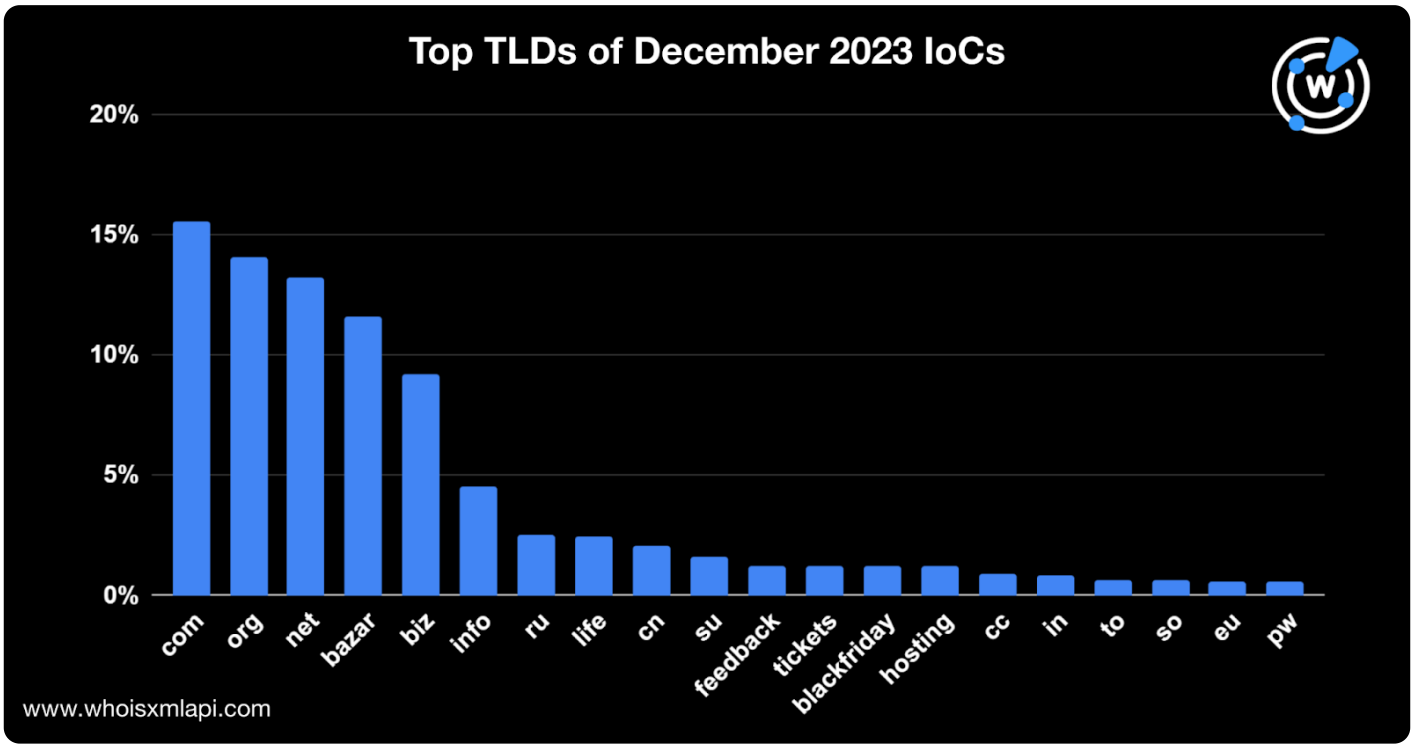
12月新注册的域名中有61%的域名未编辑过的其WHOIS记录，而39%的域名则使用了多种WHOIS隐私编辑



从DNS角度透视本月网络安全问题

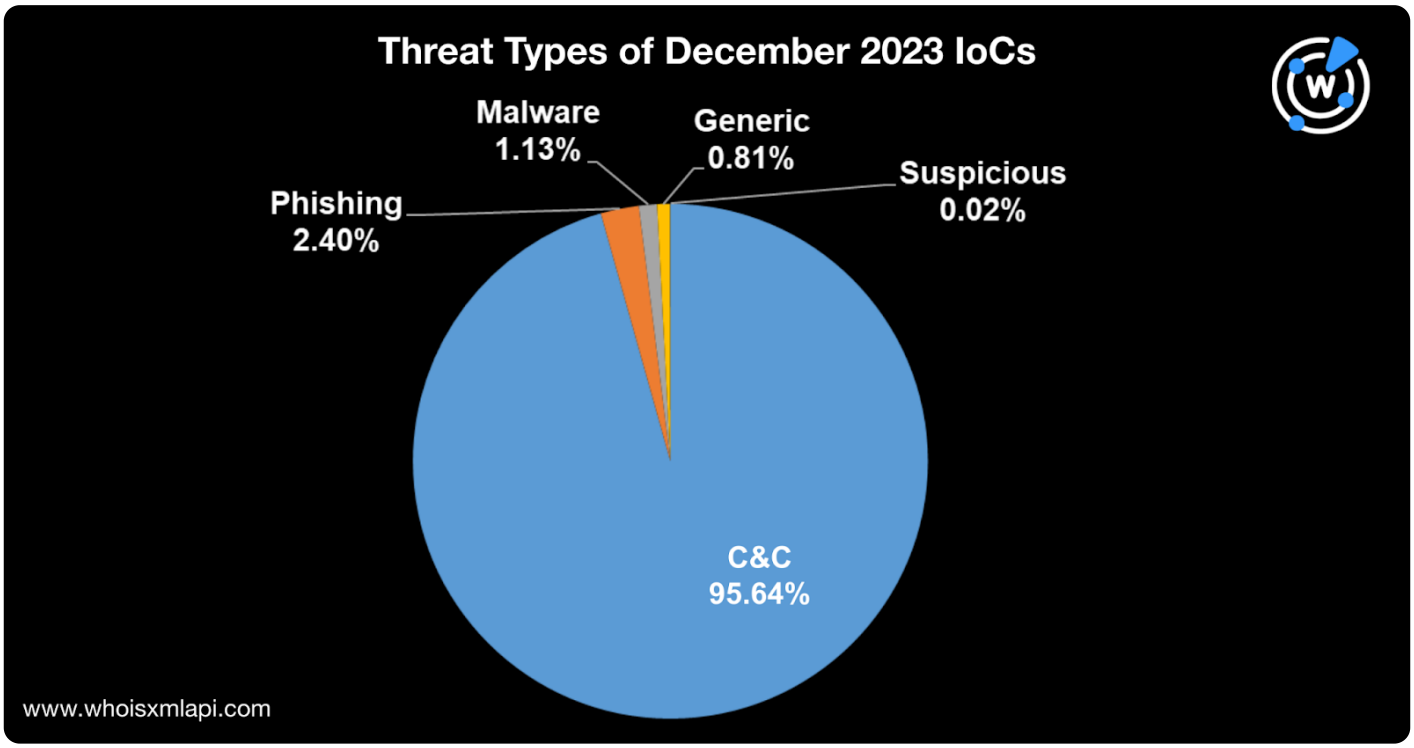
12月的IoCs中排名领先的顶级域

我们分析了12月份所监测到的150多万个IoC域名中顶级域的使用情况，发现16%的域名使用.com作为通用
(14%) 和.net
(13%)。新通用顶级域使用情况如下，12%使用了.bazar，9%使用了.biz，5%使用了.info，2%使用了.life。
(3%)、.cn 和 .su (各占比 2%)。下图显示了 IoC 排名前 20 的顶级域使用情况。



12月份IoCs威胁类型细分

我们的研究员将12月份所监测到的 IoC 按不同的威胁类型进行了分类，发现大多数 IoC 被标记为命令与控制 (C&C) 服务器类型（95.64%），2.4% 涉及网络钓鱼活动，1.13% 涉及恶意软件传播。约 0.8% 参与了其他形式的网络攻击，0.02% 被标记为可疑活动。威胁类型细分见下图。



威胁报告

以下是我们12月份所发布的相关威胁报告。

- **借助DNS情报揭露WailingCrab神秘面纱：**
  从参与WailingCrab恶意软件传播的24个妥协指标列表信息中，我们的研究人员发现了3,000多个潜在

- **窥探Atomic Stealer基础设施的“引擎盖”：** WhoisXML
  API研究人员深入研究了恶意软件Atomic
  Stealer相关联的IoCs，发现了几十个与IP和邮件地址相关联的数字资产。

- **DNS 视角下的假身份证市场：** 威胁研究员 Dancho Danchev
  发现了一个电子邮件地址，其从属于假身份证的卖家，我们的研究人员进而进行了深入调查，发现了

- **全球网络犯罪平台Genesis Market基础设施的背后：**
  深入的DNS分析：我们的研究人员发现了多个域名和 IP 地址，它们可能是 Genesis Market
  网络犯罪基础设施的一部分。

您可点击此链接查找更多报告内容。

??????????????????????????????????????