2024年1月域名事件重点回顾

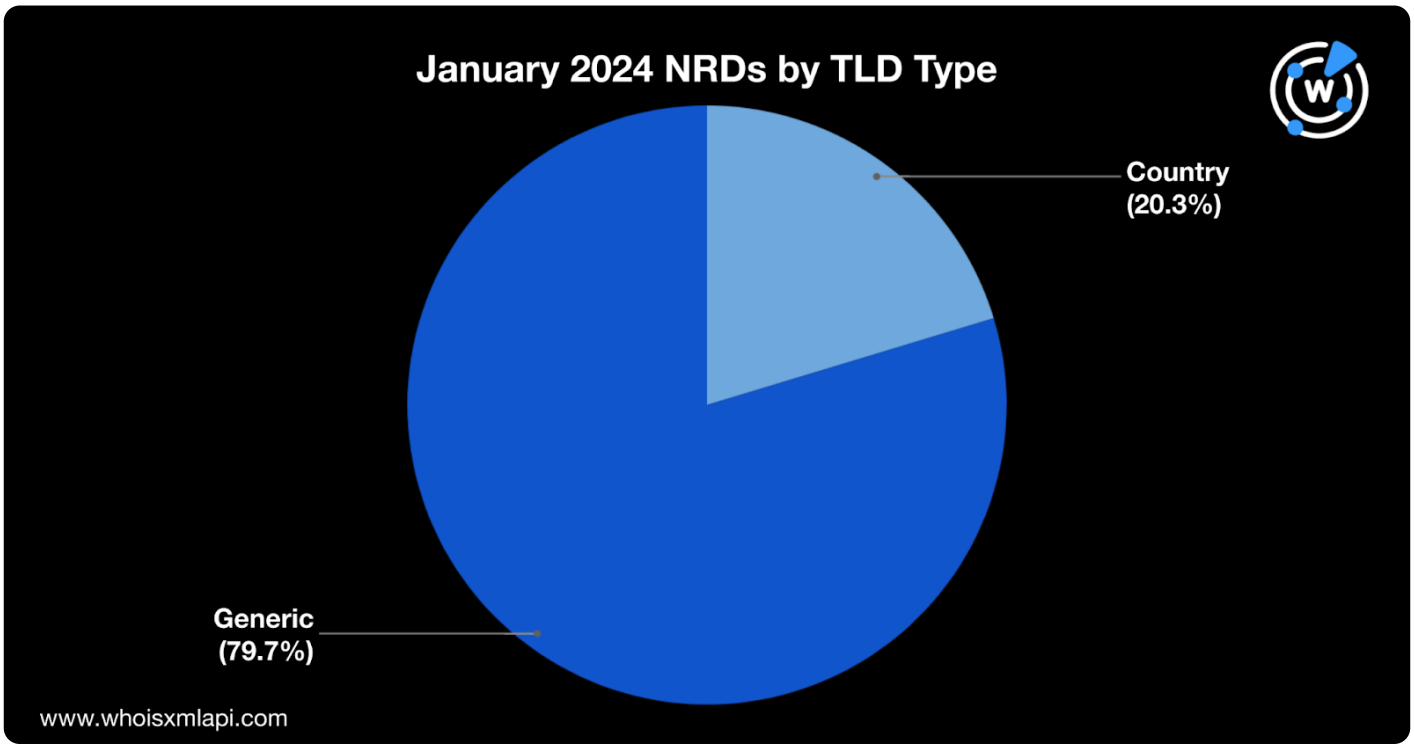
发布于 April 8, 2024

WhoisXML
API分析师选取了2024年1月1日至31日期间注册的700多万个域名作为样本进行分析，研究这些域名的发展

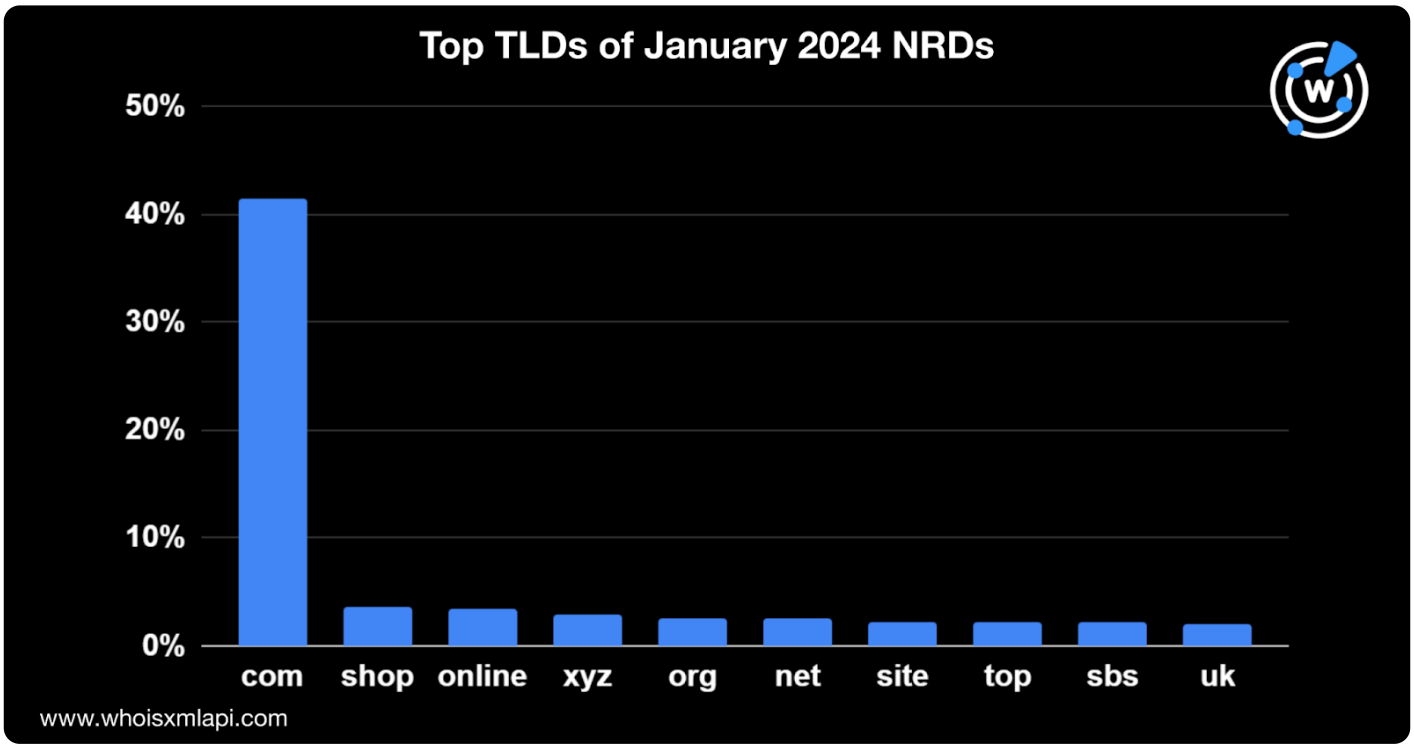
1月新注册域名详情

顶级域分布情况

2024年1月注册的700万注册域名中，通用顶级域（gTLD）占新注册域名总数的79.7%，国家代码顶级域（

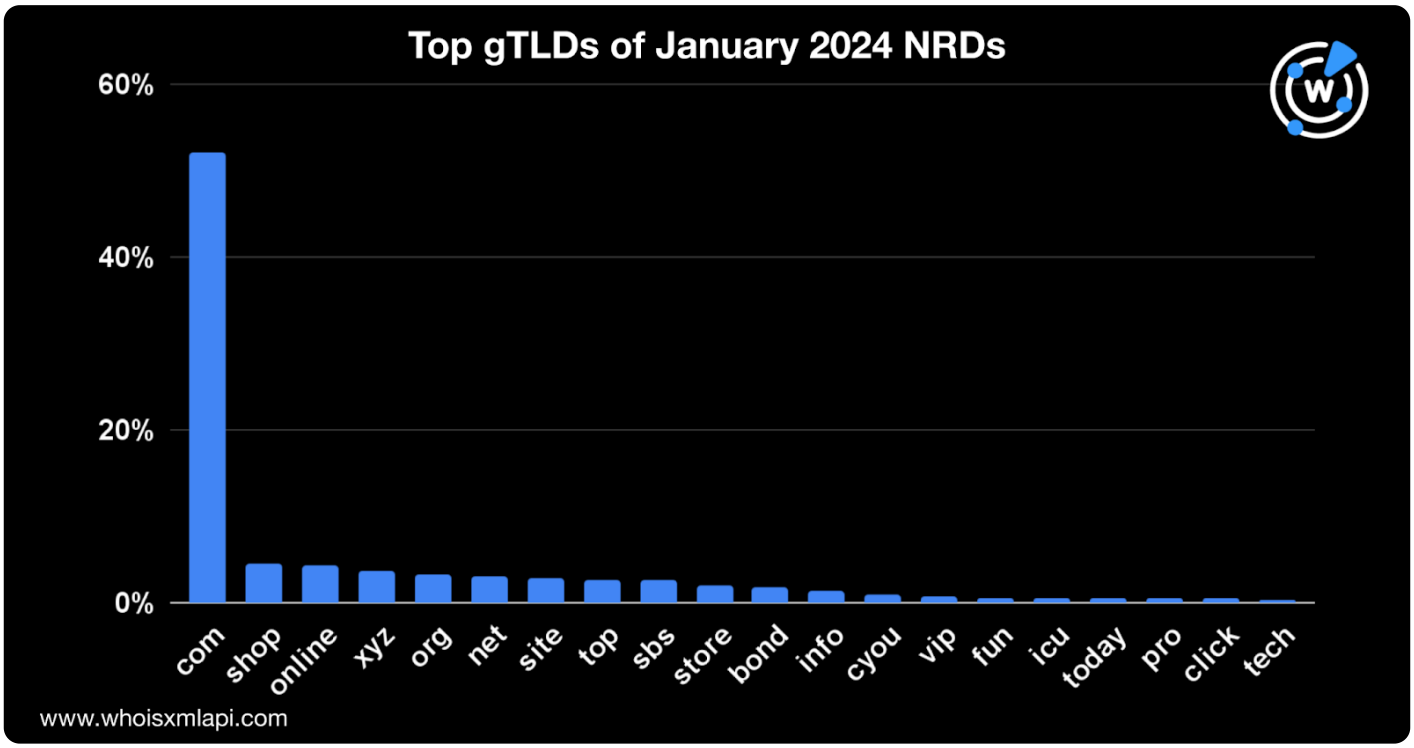


总体来说，.com顶级域后缀占新域名注册总量的41.5%，紧随其后的是.shop（占比3.6%），.online（占比
.sbs（占比2.1%）以及.uk（占比2%）。

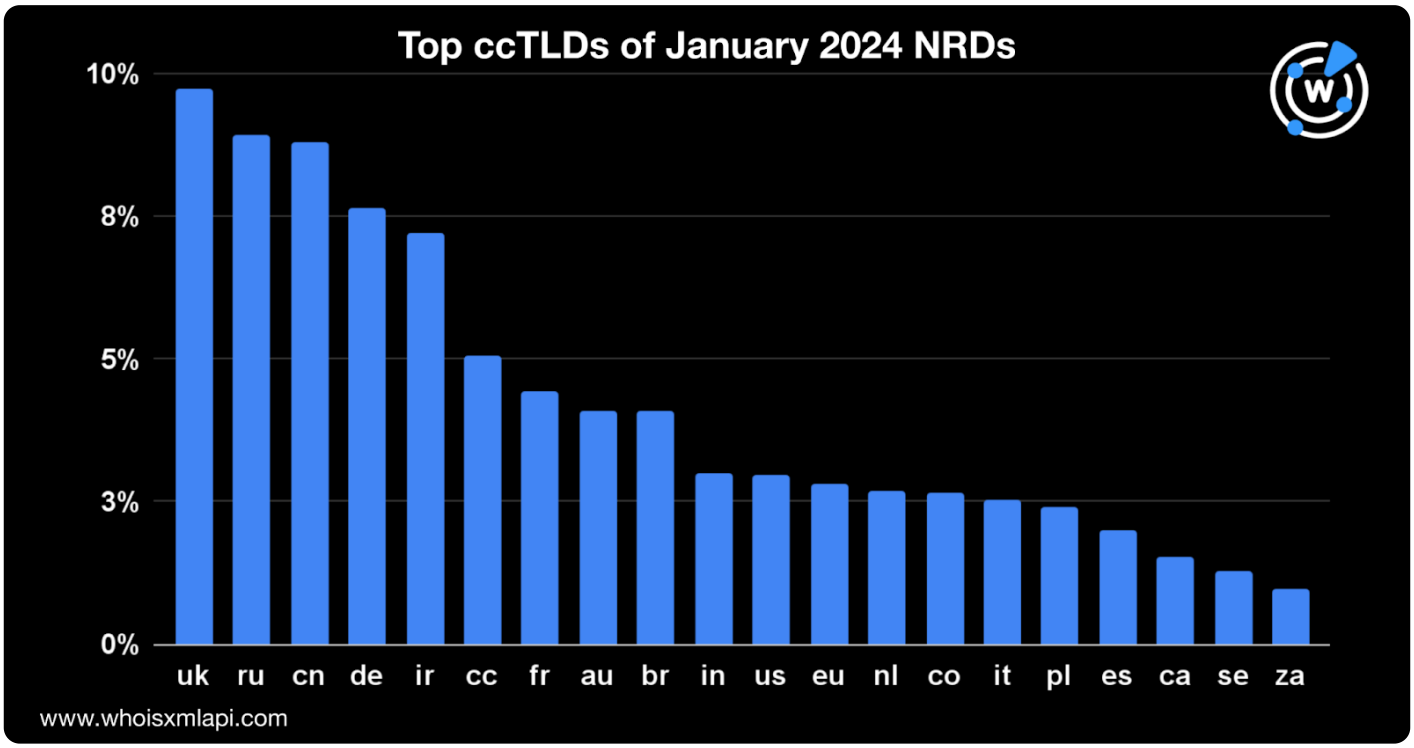


随后，我们对顶级域进行了深入分析，确定了新注册域名中最常用的通用顶级域和国家代码顶级域。

在625多种通用顶级域中，.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52.1
占比2.8%; .top和.sbs分别占比2.7%；.store占比2%; .bond占比1.8%; .info占比1.4%;
.cyou占比1%; .vip占比0.8%；.fun和.icu分别占比0.6%；.today,
.pro,和.click分别占比0.5%；.tech占比0.4%。

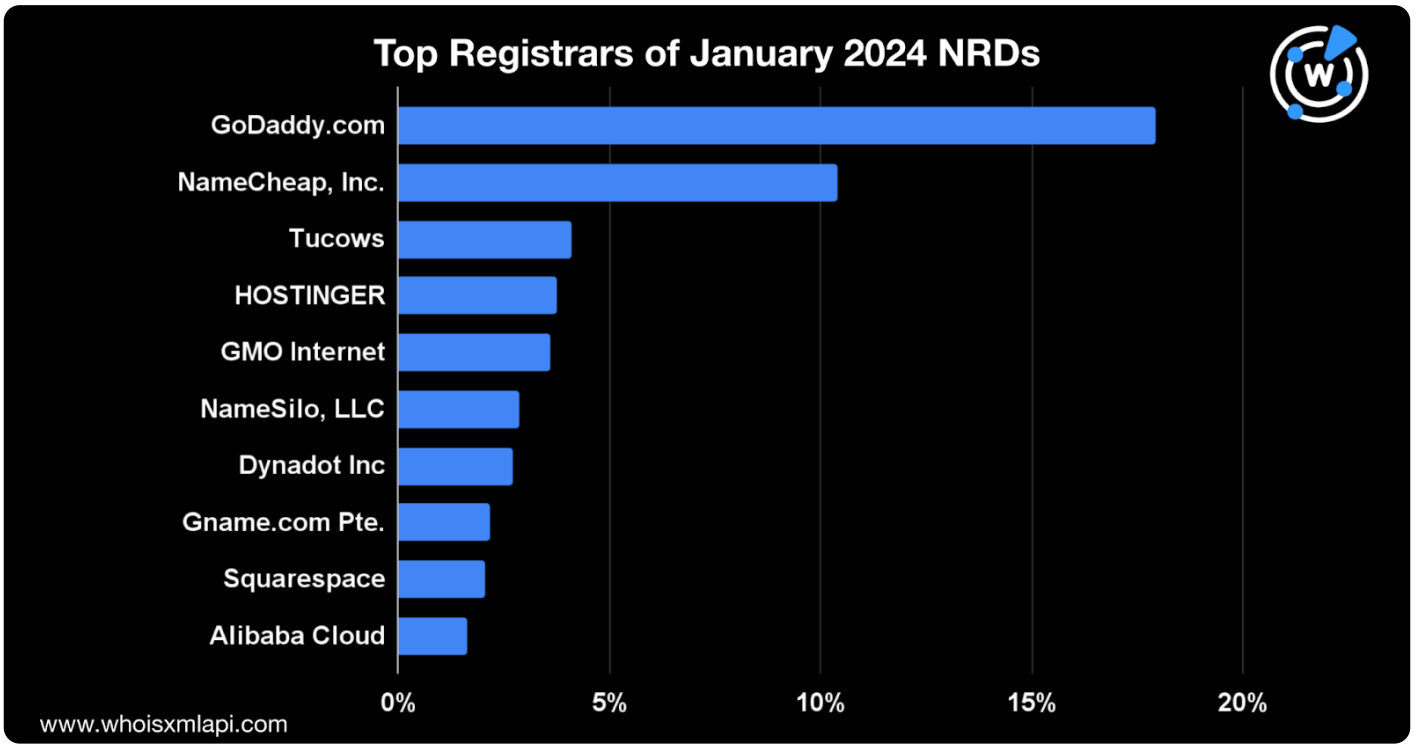


同时，在
230多个国家顶级域名中，.uk最受欢迎，占新注册域名量的9.7%。其次是.ru（占比8.9%）、.cn（占比8.8
20
的其他国家还包括.ca（占比1.5%）、.se（占比1.3%）和.za（占比1%）。这些国家顶级域占1月份新注册



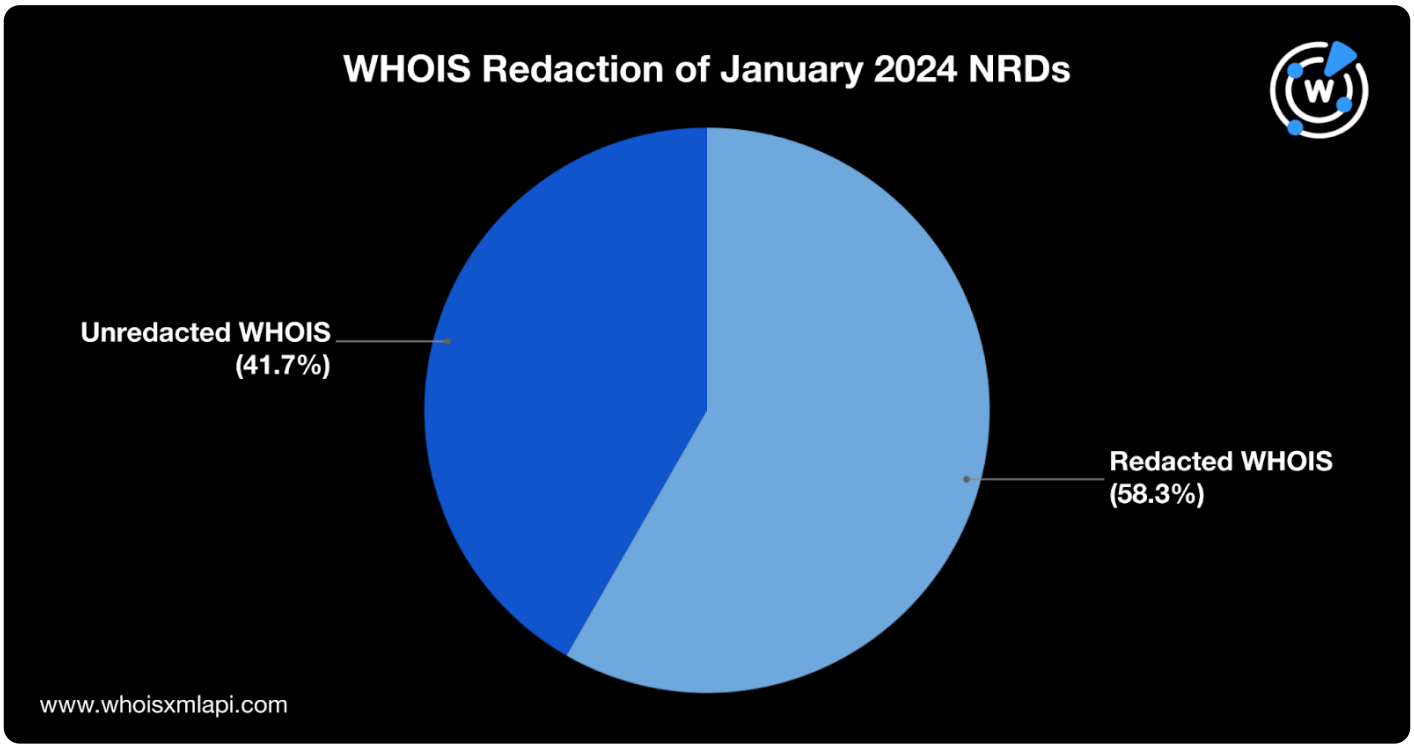
注册商分布

1月份排名领先的注册商依旧为GoDaddy和Namecheap，分别占据了新注册域名总量的18%和10.4%。剩余排名前十的注册商包括：Tucows占比4.1%，HOSTINGER占比3.8%，GMO Internet Group, Inc.占比3.6%，NameSilo LLC占比2.9%， Dynadot, Inc.占比2.7%，Gname.com Pte. Ltd.占比2.2%，Squarespace Domains LLC占比2.1%，以及阿里巴巴云计算公司占比1.6%。



WHOIS数据编辑

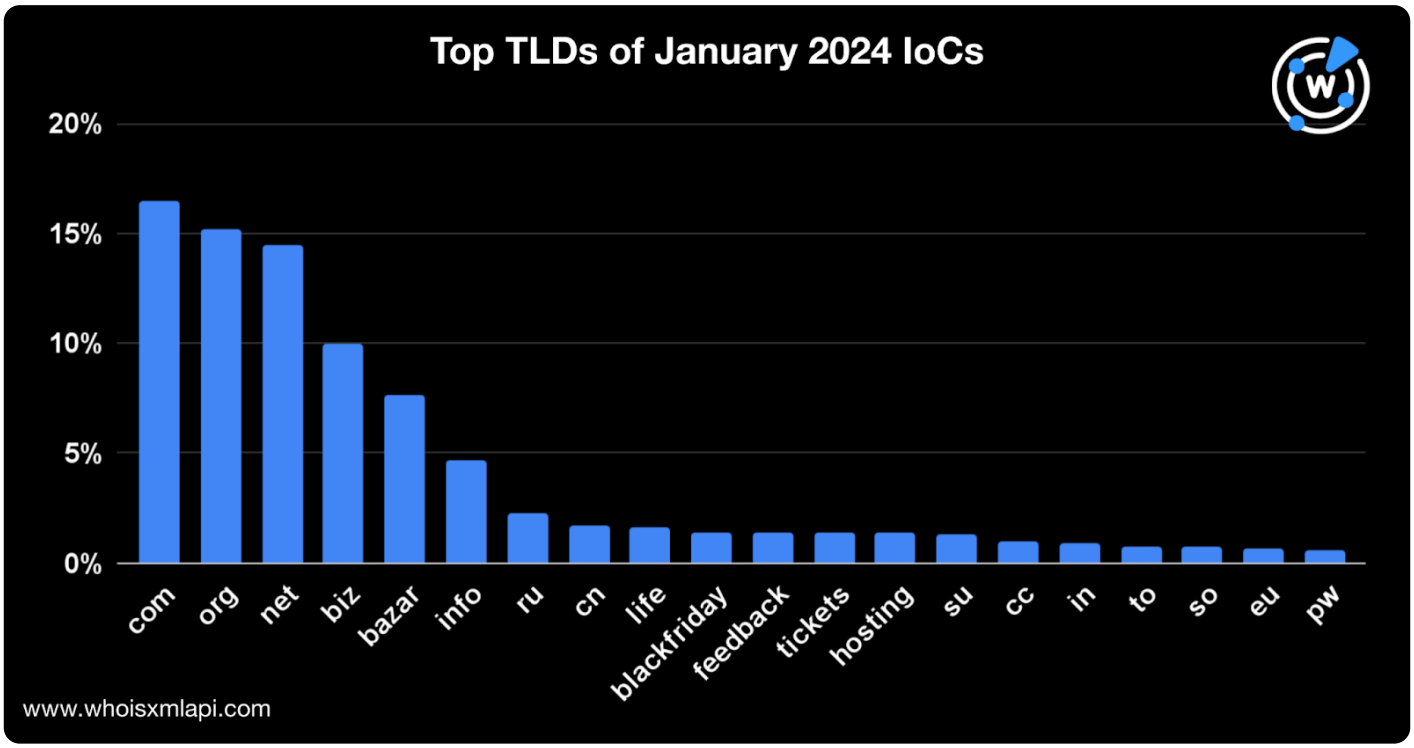
1月份新注册的域名中有58.3%的域名编辑过的其WHOIS记录，而41.7%的域名则公开其WHOIS记录。



从DNS角度透视本月网络安全问题

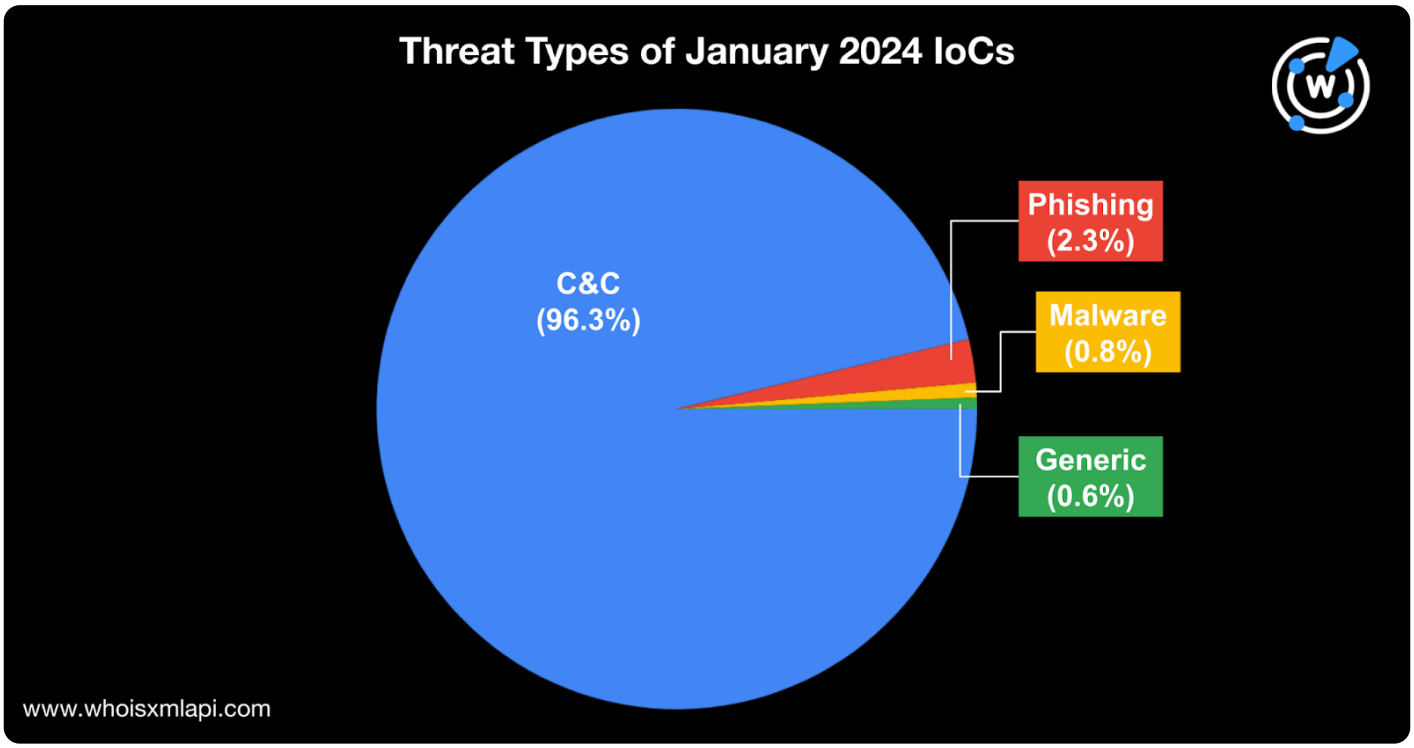
1月的IoCs中排名领先的顶级域

我们分析了1月份所监测到的110多万个IoC域名中顶级域的使用情况，.com 是 IoC
中最常用的通用顶级域扩展名，占恶意域名的
16.5%。紧随其后的主要通用顶级域为.org占比15.2%，.net占比14.4%，以及.biz占比10%。其他IoC所使



1月份IoCs威胁类型细分

我们将1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（96.3%），2.3% 涉及网络钓鱼活动，0.8% 涉及恶意软件传播。约 0.6% 参与了其他形式的网络攻击。威胁类型细分见下图



威胁报告

以下是我们1月份所发布的相关威胁报告。

- 利用 DNS情报探索 Epsilon Stealer的相关痕迹：WhoisXML API 研究团队在与 Epsilon Stealer 相关的 133 个妥协指标 (IoC) 中提取了 76 个域名列表，发现了 1,700 多个可能相关的数字化记录信息
- 窥探 PikaBot 基础设施：与恶意广告传播相关的PikaBot 的 11 个 IoC 列表中，我们的研究人员发现了数百个与电子邮件和 IP相关联的数字化记录信息。
- 调查 UNC2975 恶意广告活动基础设施：我们分析了与 UNC2975 恶意广告活动相关的 28 个 IoC，发现了 3,000 多个潜在关联的数字化信息。

您可点击此链接查找更多报告内容。

??