2024年2月域名事件重点回顾

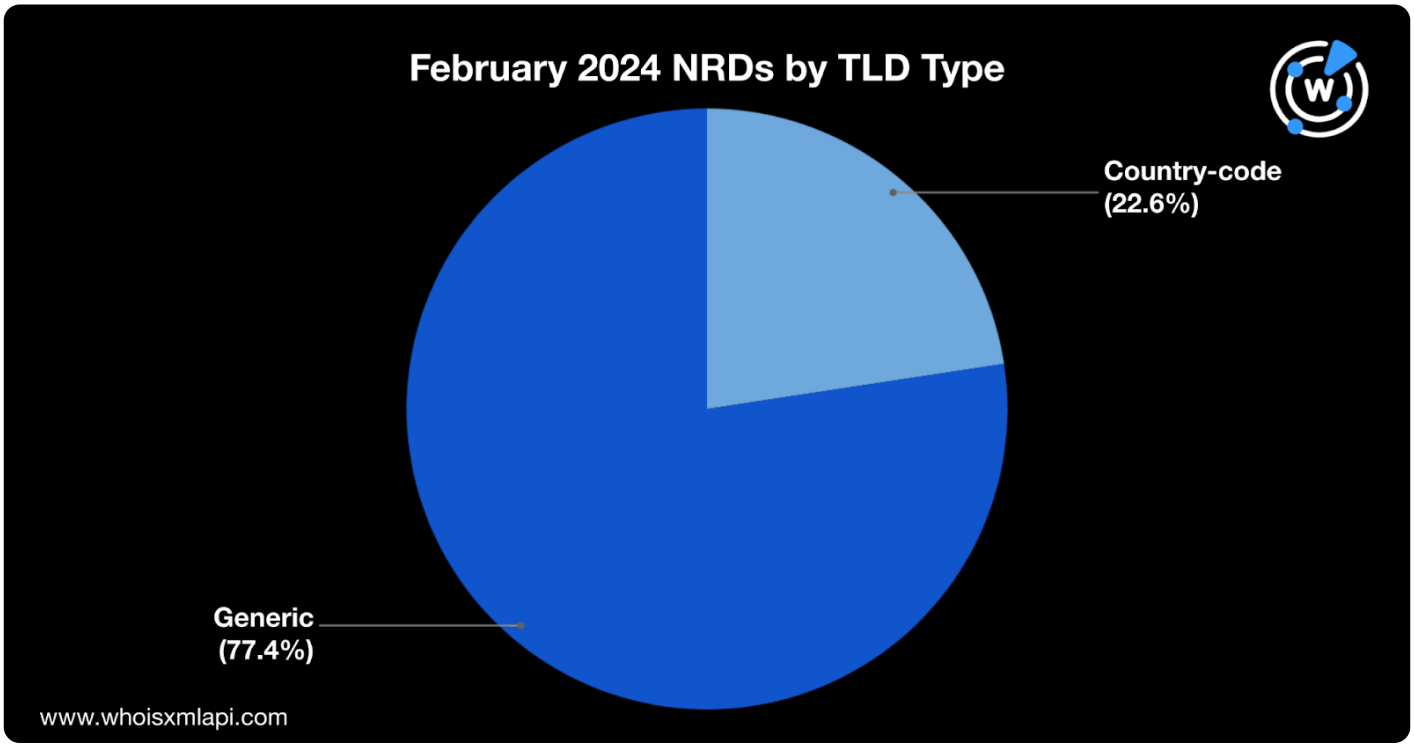
发布于 April 8, 2024

WhoisXML
API分析师选取了2024年2月1日至29日期间注册的660多万个域名作为样本进行分析，研究这些域名的发展

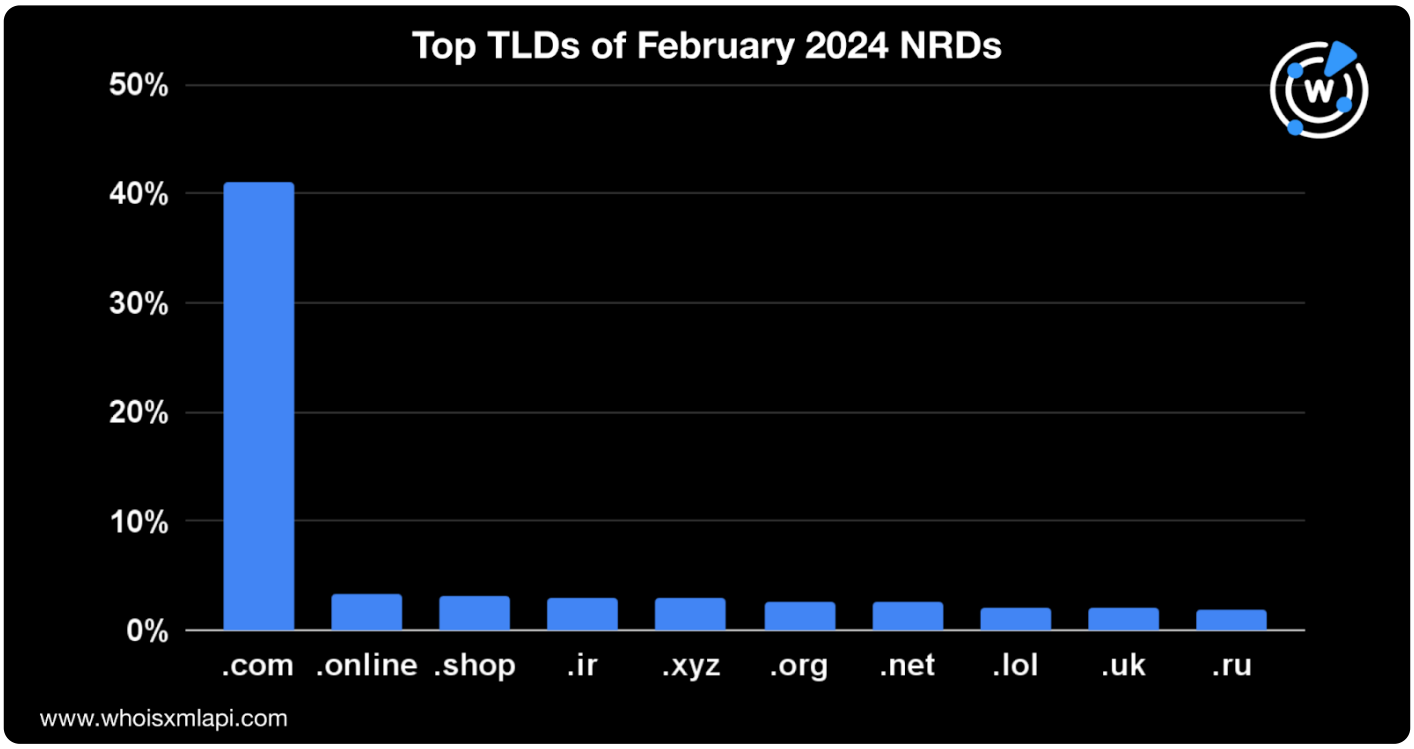
2月新注册域名详情

顶级域分布情况

2024年2月注册的660万注册域名中，通用顶级域（gTLD）占新注册域名总数的77.4%，国家代码顶级域（



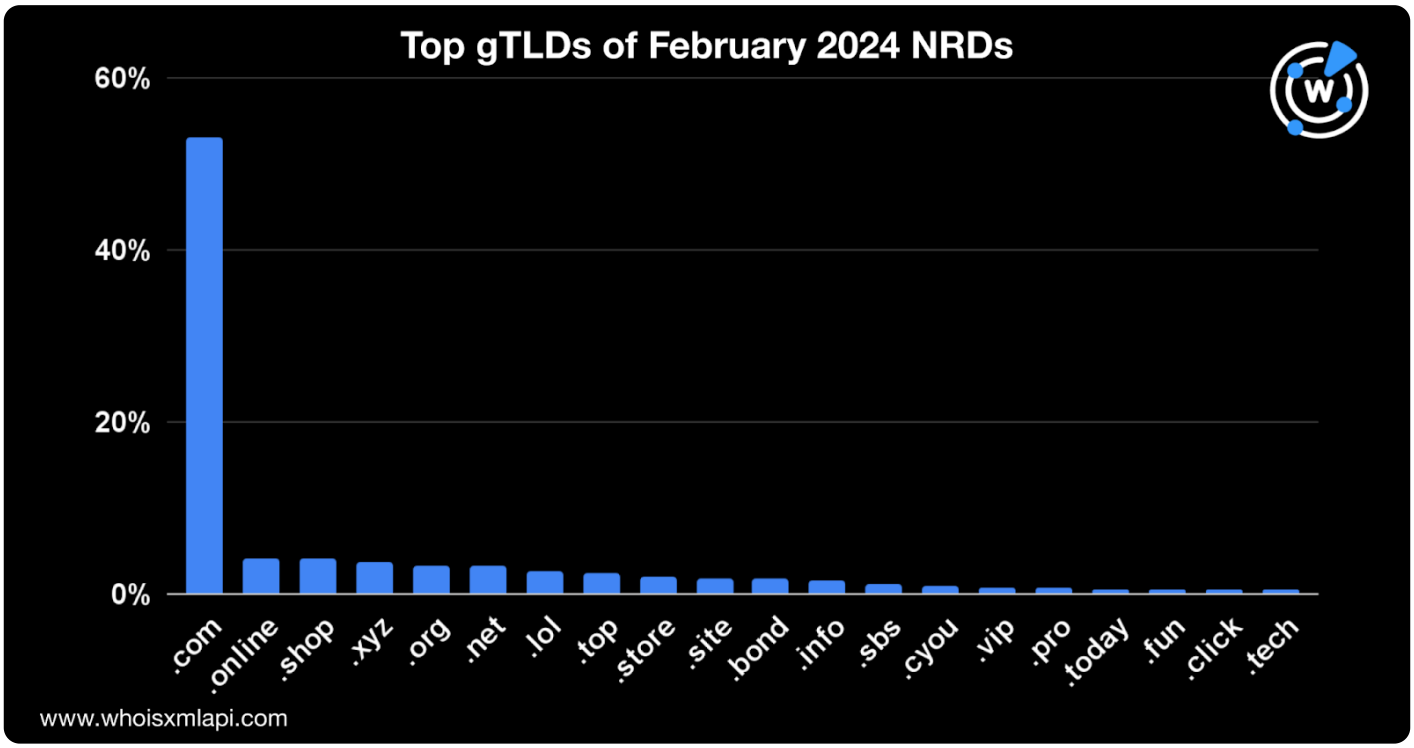
与前几个月情况相同，.com使用最为频繁，占新域名注册总量的41.1%，紧随其后的是.online（占比3.3%）.uk和.ru分别占比2%。



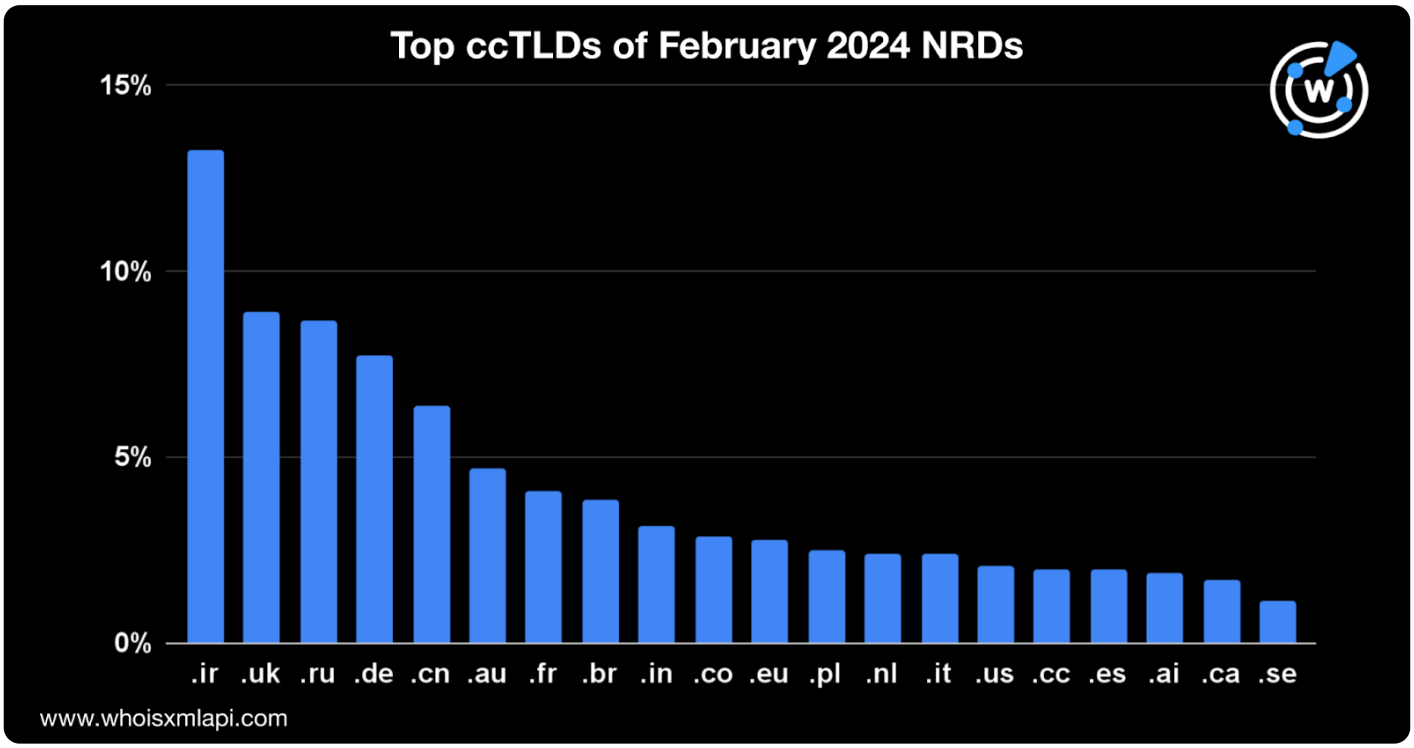
随后，我们对顶级域进行了深入分析，确定了新注册域名中最常用的依旧是通用顶级域和国家代码顶级域。

在640多种通用顶级域中，.com占所有通用顶级域的新注册域名总数的53.1%。剩余排名前20的顶级域相差

例如，与电子商务相关的通用顶级域 .online 和 .shop 分别占比4.2%位居第二；.xyz 为 3.7%；.org 为 3.4%；.net 为 3.3%；.lol 为 2.6%；.top 为 2.5%；.store 为 2.1%；.site 为 1.9%；.bond 为 1.8%；.info 为 1.5%；.bs 为 1.1%；.cyou 为 1%；.vip 为 0.8%。store 占 2.1%；.site 占 1.9%；.bond 占 1.8%；.info 占 1.5%；.sbs 占 1.1%；.cyou 占 1%；.vip 占 0.8%；.pro 占 0.7%；.today、.fun 和 .click 各占 0.5%；.tech 占 0.4%。

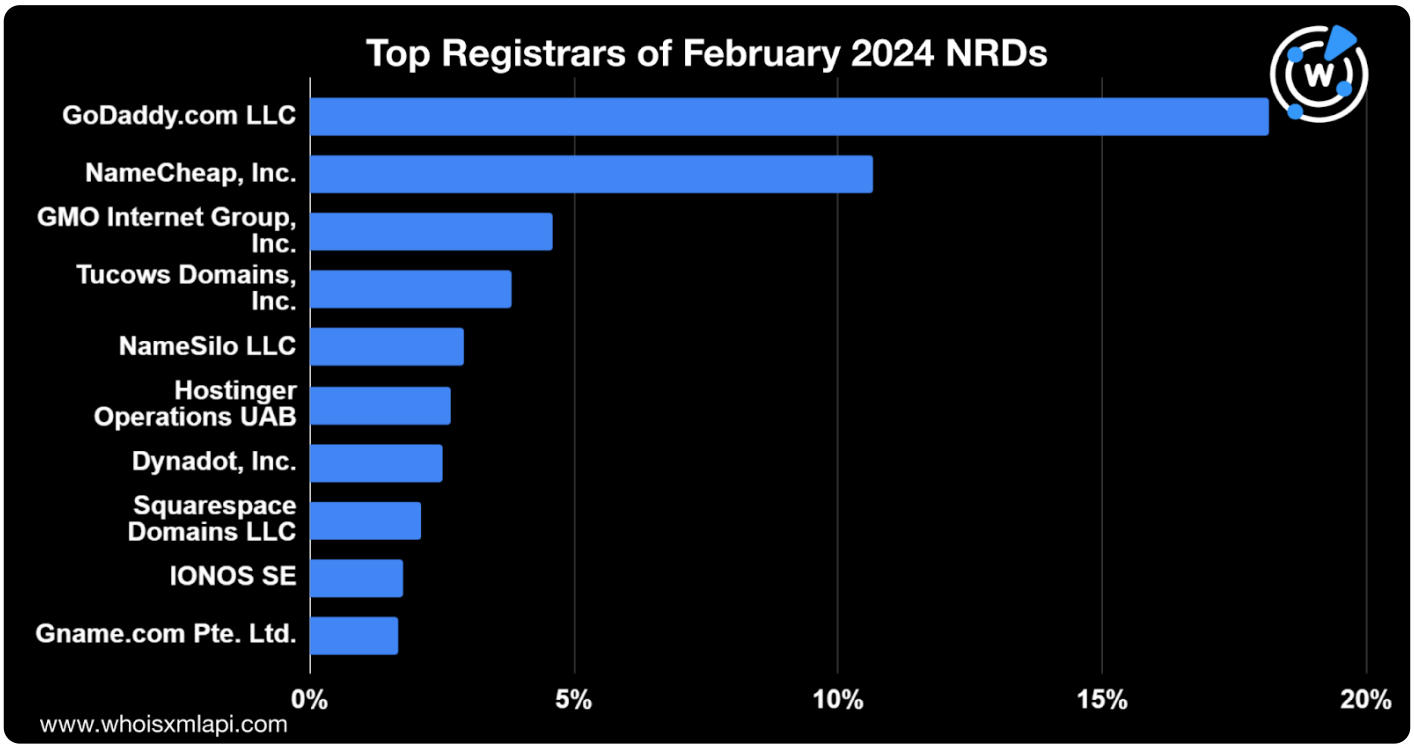


同时，在
230多个国家顶级域名中，.uk最受欢迎，占新注册域名量的9.7%。其次是.ru（占比8.9%）、.cn（占比8.8
20
的其他国家还包括.ca（占比1.5%）、.se（占比1.3%）和.za（占比1%）。这些国家顶级域占1月份新注册



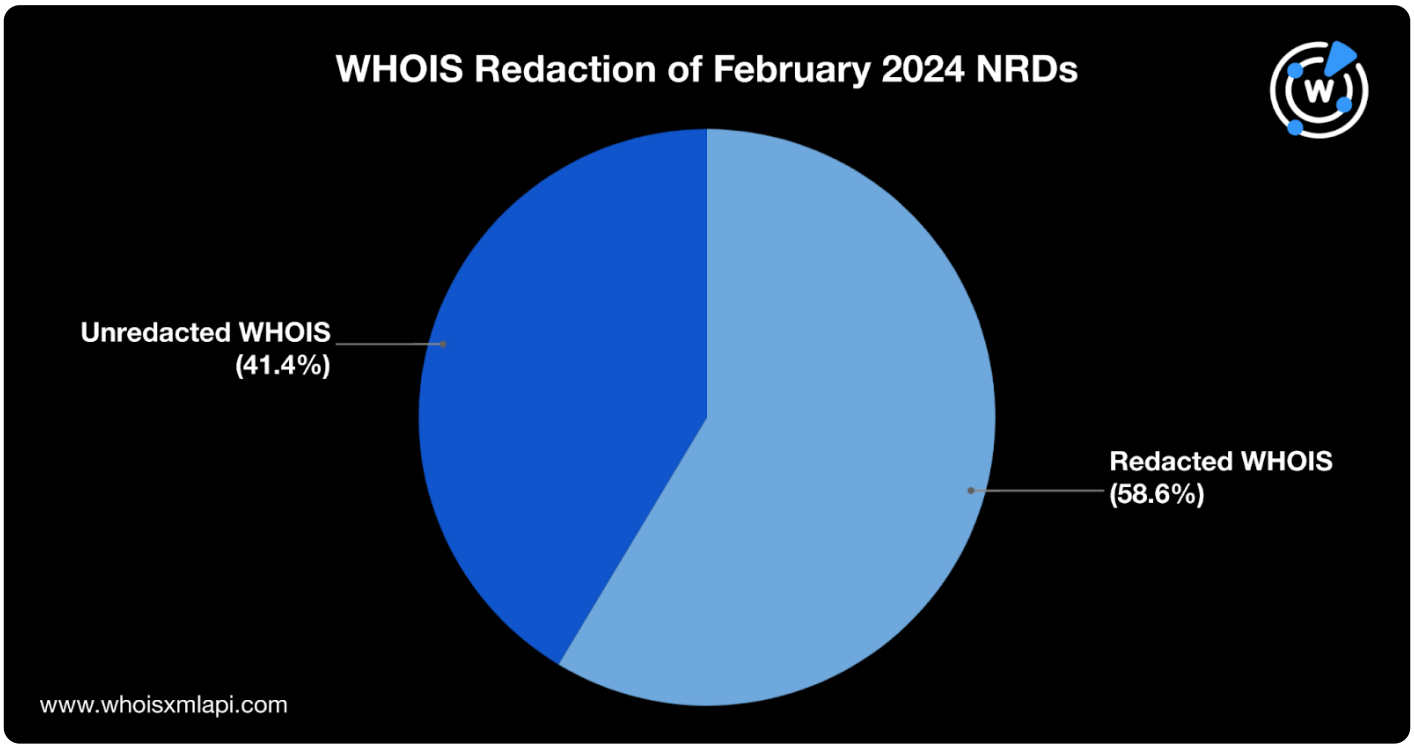
注册商分布

2月份排名领先的注册商依旧为GoDaddy，占新注册域名总量的18.1%，紧随其后的是Namecheap，占比1
Internet Group, Inc.，占比4.6%；Tucows Domains,
Inc.，占比3.8%。。剩余排名前十的注册商包括：NameSilo LLC（占比2.9%）、Hostinger
Operations UAB（占比2.7%）、Dynadot, Inc.（占比2.5%）、Squarespace Domains
LLC（占比2.1%）、IONOS SE（占比1.8%）和 Gname.com Pte. Ltd. (占比1.7%)。



WHOIS数据编辑

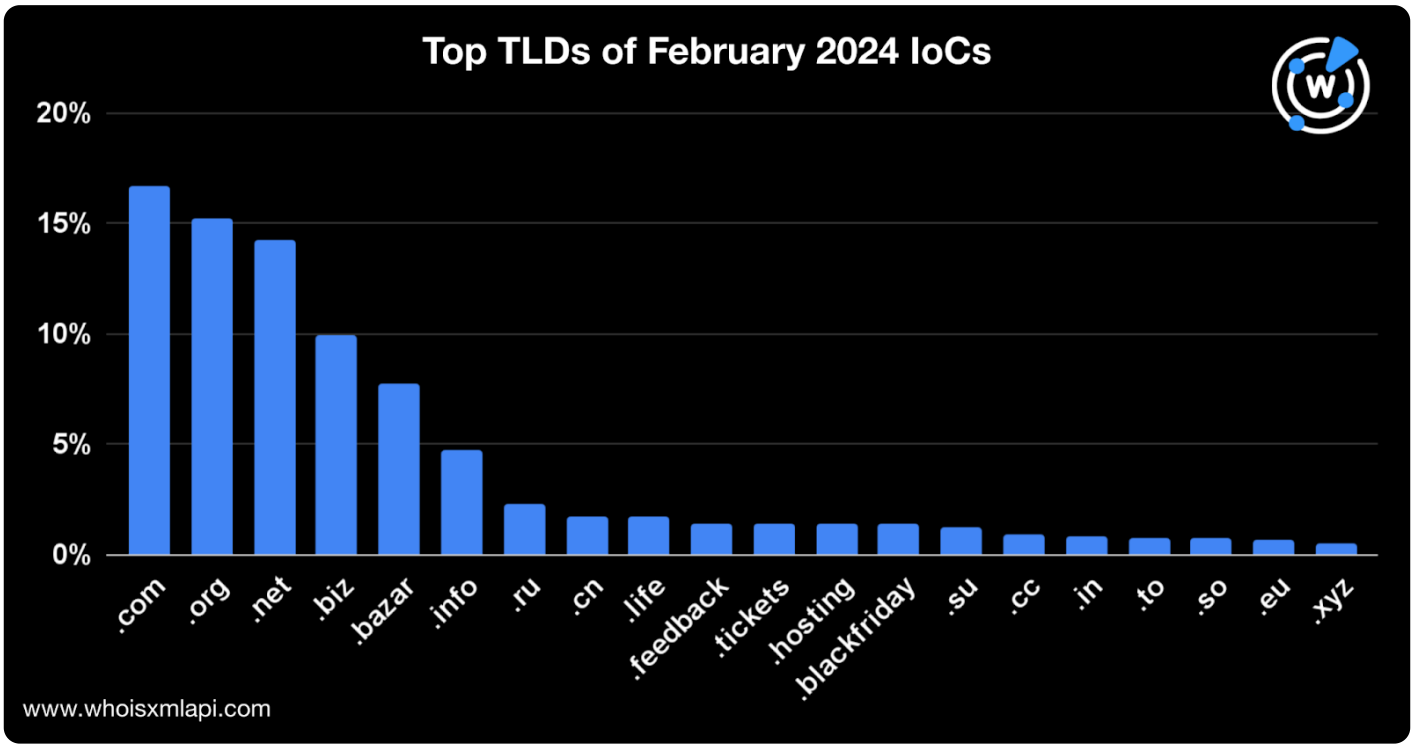
2月份新注册的域名中有58.6%的域名有隐私保护的WHOIS数据，而41.4%的域名则公开其WHOIS记录。



从DNS角度透视本月网络安全问题

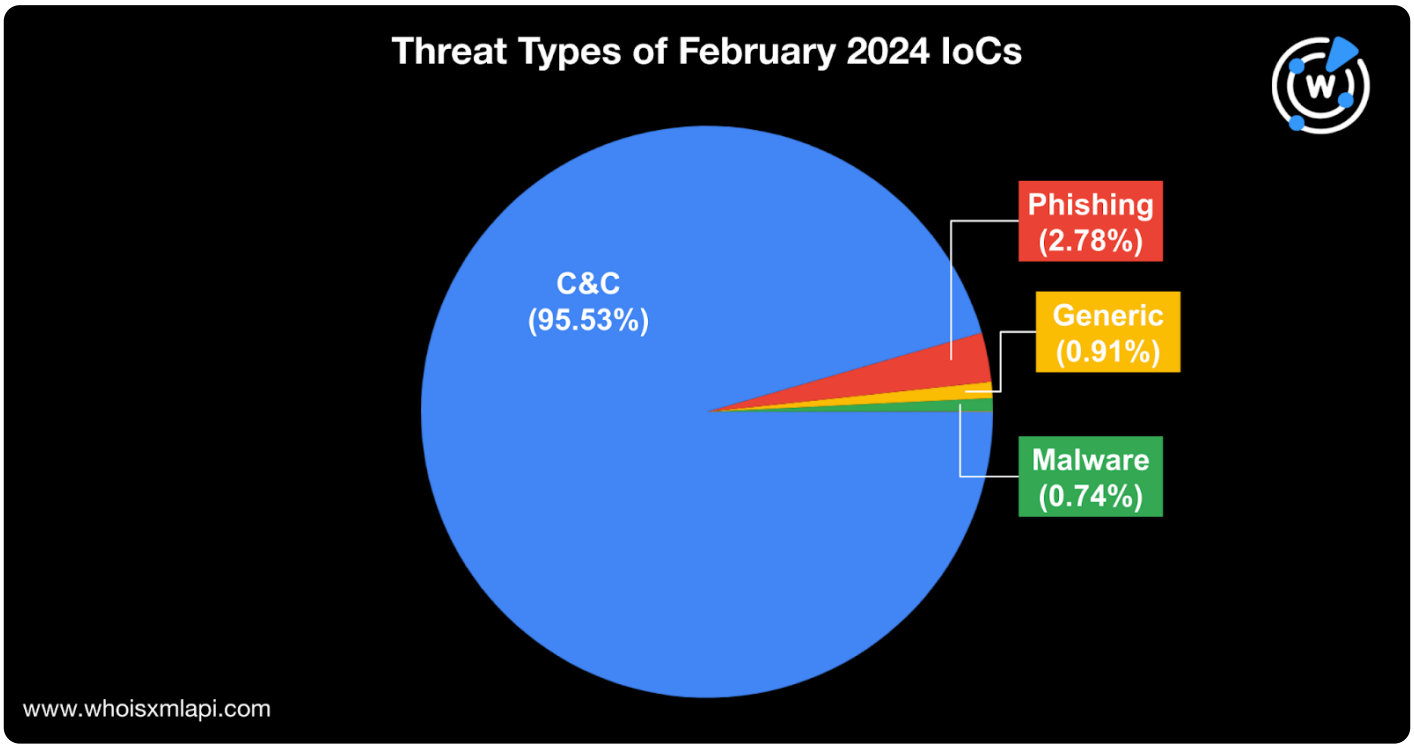
2月的IoCs中排名领先的顶级域

我们分析了2月份所监测到的100多万个被标记为IoC的域名使用情况，.com 是 IoC
中最常用的通用顶级域扩展名，占恶意域名的
16.6%。紧随其后的主要通用顶级域为.org占比15.2%，.net占比14.3%，以及.biz占比10%。一些IoC所使



2月份IoCs威胁类型细分

我们将2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（95.53%），2.78% 涉及网络钓鱼活动，0.74% 涉及恶意软件传播，约 0.91% 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2月份所发布的相关威胁报告。

- 在 DNS 中追踪 Ivanti 零日漏洞IoC：从与 Ivanti 产品漏洞相关的 20 个 IoC 列表中，我们的研究团队发现了 397 个潜在数字资产，它们与 IoC共享电子邮件地址、IP 决议和字符串用法。
- DNS 调查：xDedic 被取缔后是否真的完结了？WhoisXML API 研究团队对 19 个 xDedic IoC 进行了扩展分析，即使在执法人员关闭网络犯罪即服务 (CaaS) 市场之后，依然发现了150 个与电子邮件、IP 和字符串相关联的数字资产
- DNS 深度挖掘杀猪骗局：通过分析 8 个 IoC，我们调查了所谓的 "杀猪 "新骗局，导向了 141 个与之相关的数字资产。
- DNS 聚焦下的新 RisePro 版本：我们的研究人员调查了与新检测到的 RisePro 变种相关的 10 个 IoC，发现了数百个潜在的数字资产，其中许多都是恶意的。

您可点击此链接查找更多报告内容。

??