2023年4月域名事件重点回顾

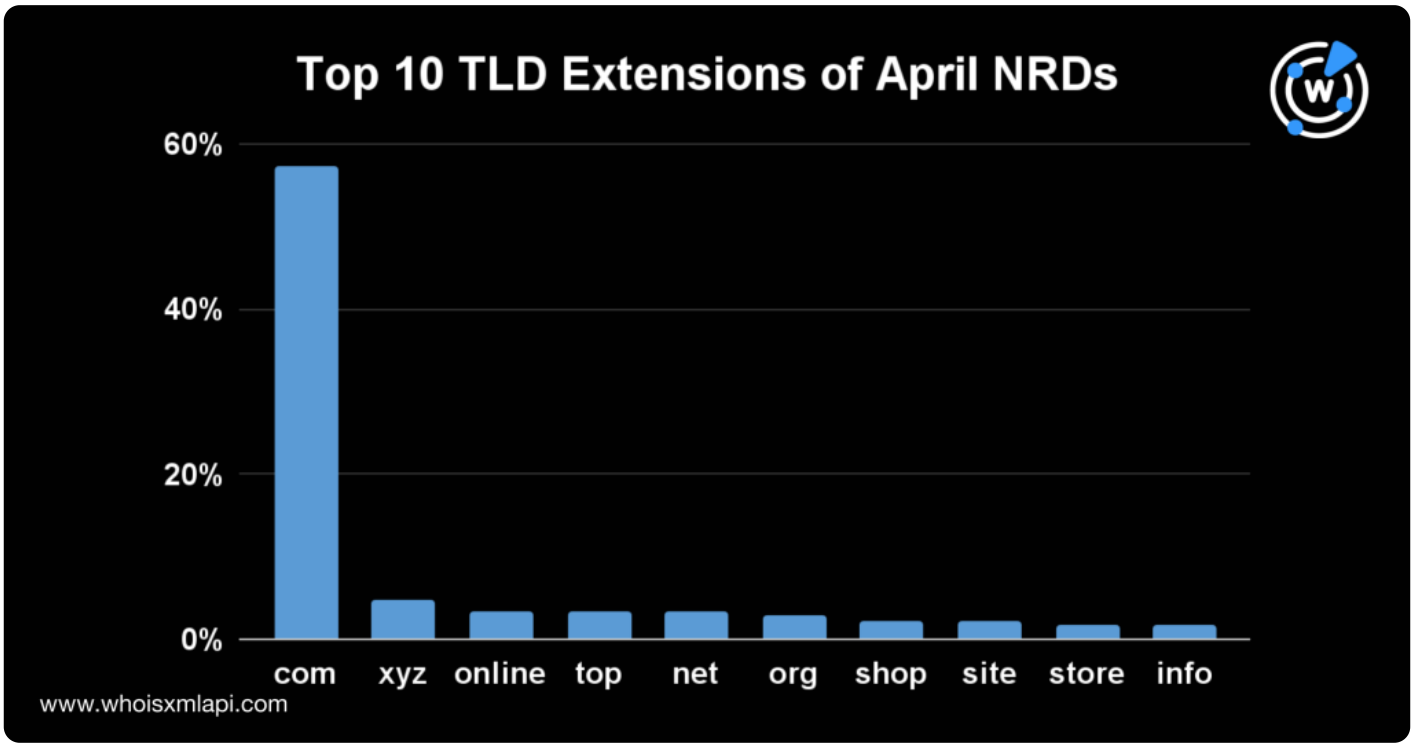
发布于 May 30, 2023

2023年4月1日-30日期间域名注册约数百万，WhoisXML
API分析师从中随机选取了29,000个域名作为样本进行分析，研究这些域名的顶级域、注册商、注册国家分

4????????

顶级域分布情况

顶级域.com依旧是使用频率最高的域名，占4月份域名注册总量的57%，紧随其后的是.xyz（占比5%），.
.top, .net, 和
.org（分别占比3%），.info占比2%。专注于电子商务的.shop，.site以及.store也排名在前十中，分别占比

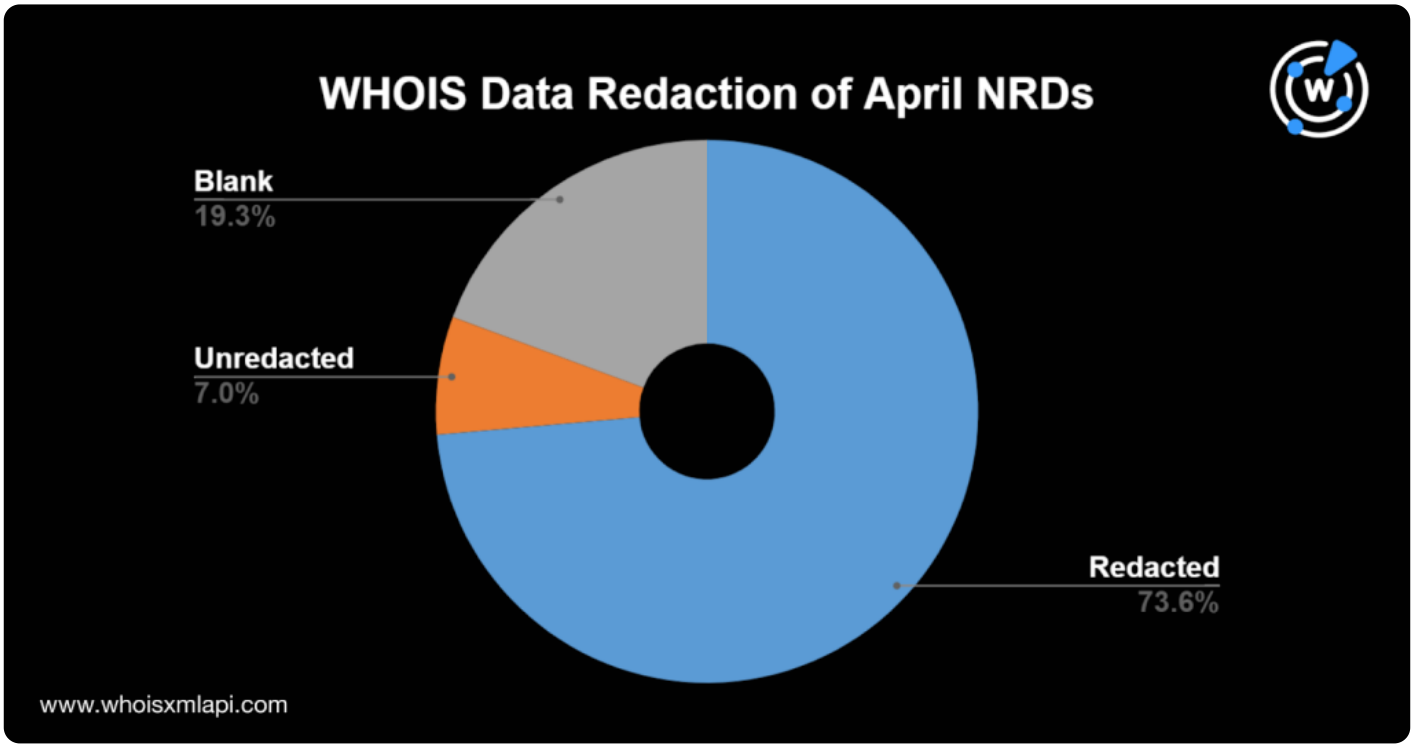


根据Infoblox在《2022年网络威胁报告》中的内容显示，4月份新增注册域名中有11.4%具有通用顶级域扩展

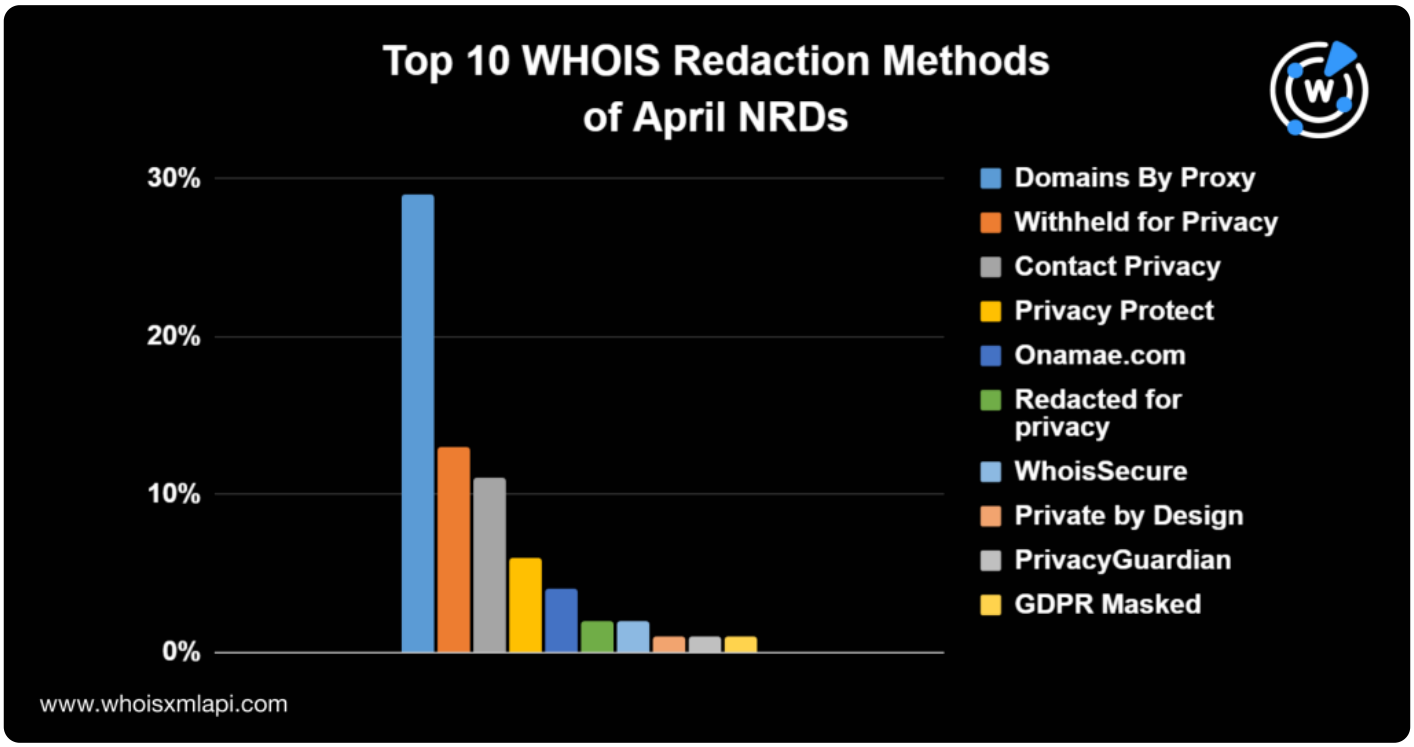
顶级域名	域名注册量占比4月份NRD注册总量
.xyz	4.785%
.top	3.395%
.click	0.724%
.buzz	0.613%
.live	0.501%

WHOIS 数据编辑

基于新注册域名注册机构信息，74%的机构编辑过其WHOIS信息，对比上月数据略有下降。约有19%的注册

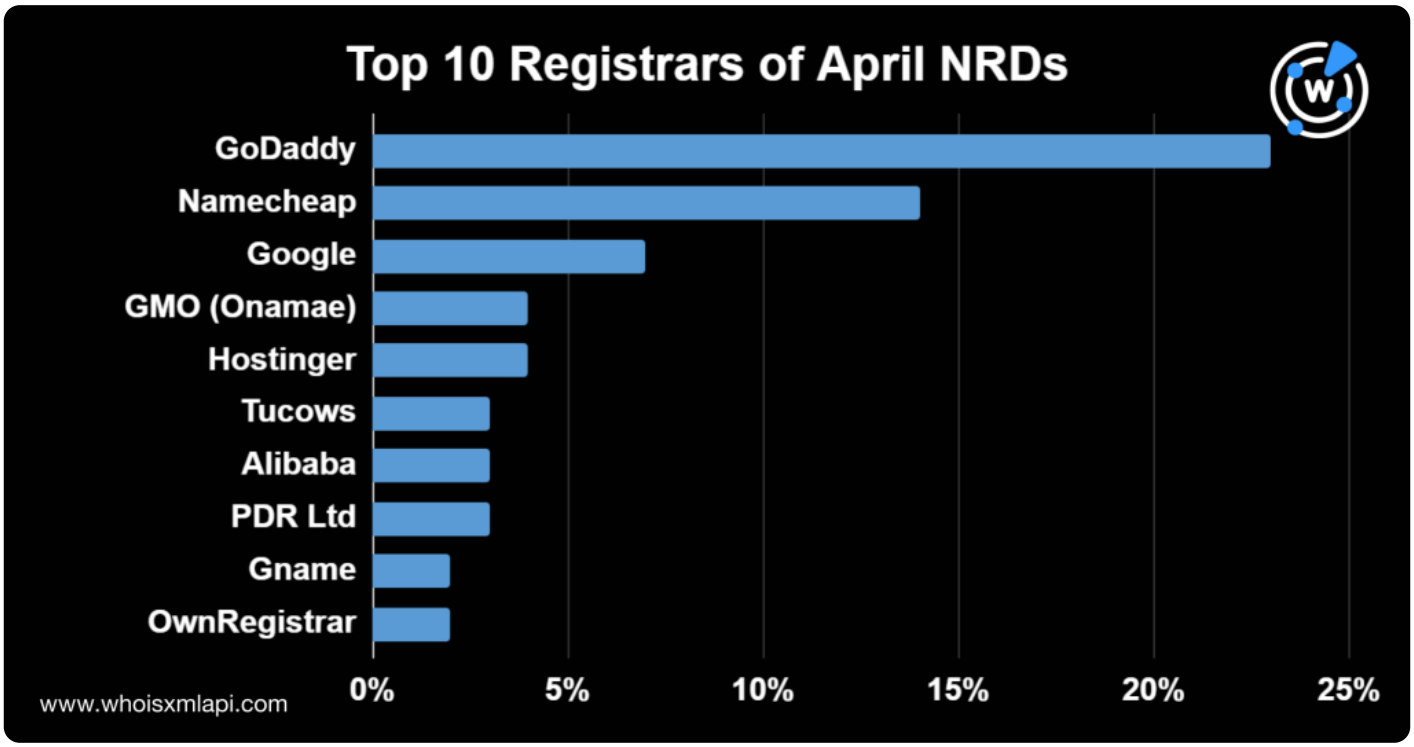


Domains By
Proxy是排名第一的WHOIS隐私保护服务提供商，拥有30%的份额，紧随其后的是Withheld for Privacy EHF，占比约13%，Contact Privacy, Inc. ，占比约为8%，Privacy Protect LLC ，占比约为6%。下表则是最常用的排名前十的数据编辑服务提供商。



注册商分布

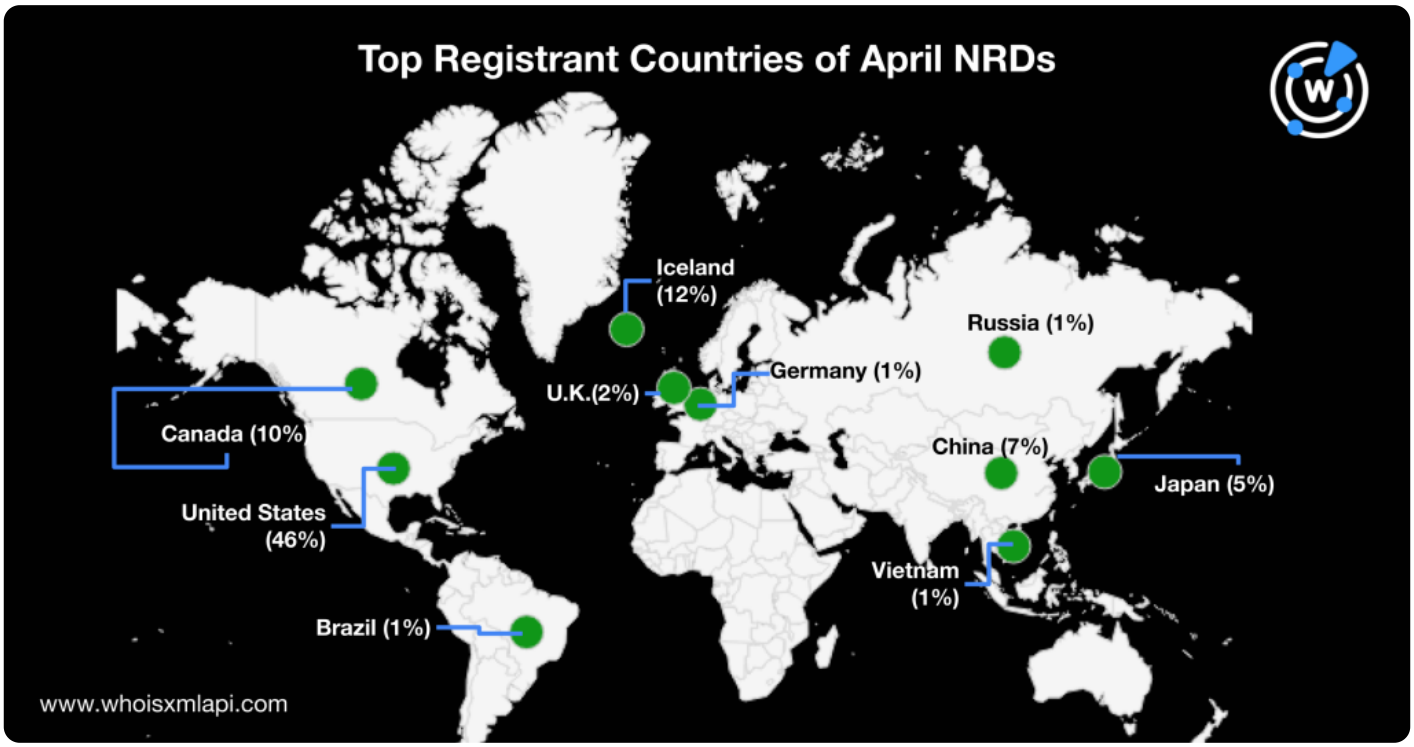
2023年4月，GoDaddy依旧是排名第一的注册商，占域名注册总量的23%，排名第二的注册商是Namecheap和GMO Internet （分别占比4% ）, Tucows (3%)，阿里巴巴 (3%), PDR Ltd. (3%), Gname.com (2%)，以及OwnRegistrar (2%)。



排名前十的注册商域名数量占域名总域名注册量的63%，其余的域名则分布在其他的350家注册商中。

排名领先的注册国家

四月份新增注册域名中有46%的域名是在美国注册的，而冰岛和加拿大注册的数量分别为12%和10%。四月



二级域名中常见的字符串

Xn仍然是这几个月来最常用的文本字符串之一，国际化域名（IDNs）也持续热门。此外，字符串如app和a

此外，game，bet，best和job这些词也频繁使用。常见的字符串详见下图词云。

?DNS????????????

以下是我们4月份所发布的相关威胁报告。

- **透过DNS揭秘潜在的商业电子邮件诈骗工具**：WhoisXML
  API研究人员分析了专门针对高官人员的商业电子邮件泄密（BEC）诈骗事件相关的公开的妥协指标（

- **在DNS中寻找针对社交媒体网红的诈骗痕迹**
  ：我们的研究人员在针对社交媒体网红或政治人物的冒充性恶意活动中发现了1600多个相关的域名。

- **揭露专门针对拉丁美洲和加勒比地区的欺诈手段**
  ：我们重点关注了针对拉丁美洲和加勒比地区的欺诈行为，发现了近10,000多个针对该地区航空和数字

- **透过DNS追踪区分SYS01和Ducktail**
  ：我们重点研究了两款恶意软件SYS01和Ducktail基于DNS的共性，两者近期都有针对脸书业务的商家

- **对Black Basta勒索软件的DNS调查发现了OneNote和Courier的冒充**：WhoisXML
  API的研究人员对Black
  Basta勒索软件相关的妥协指标进行调查时发现了近1000多个域名与这些IoCs共享WHOIS基础设施，其

点击此处可阅读更多报告内容。

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