2023年5月域名事件重点回顾

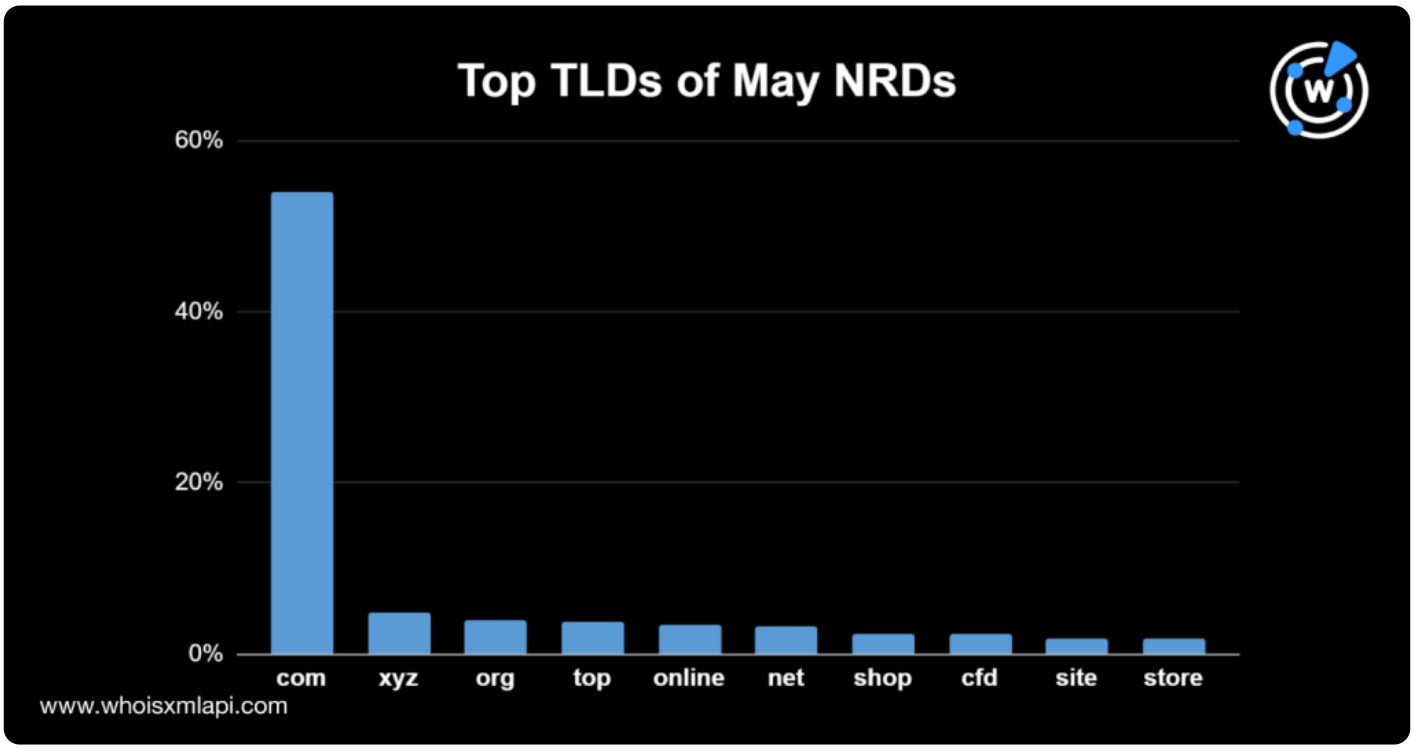
发布于 June 13, 2023

2023年5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31,000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

5月新注册域名详情

顶级域分布情况

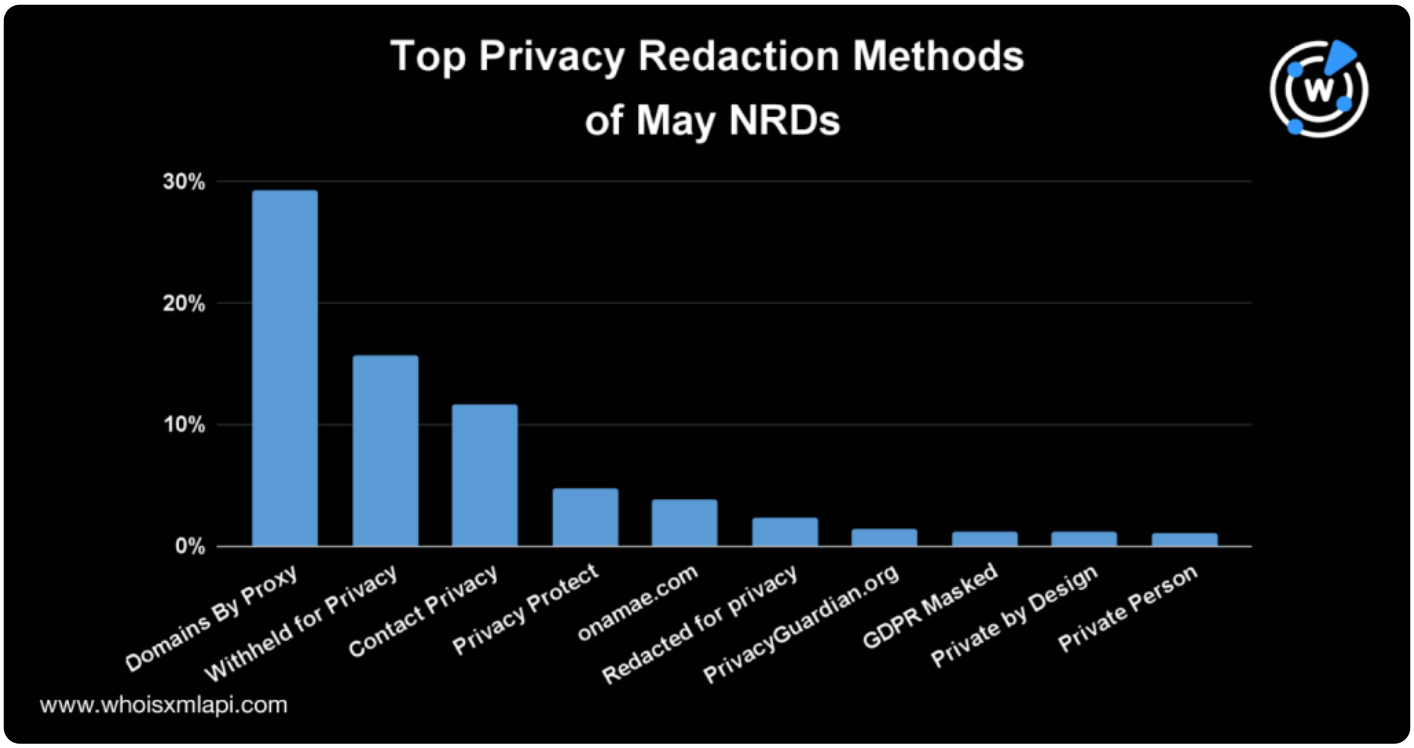
顶级域.com依旧是使用频率最高的域名，占4月份域名注册总量的54%，紧随其后的是.xyz（占比5%），.c



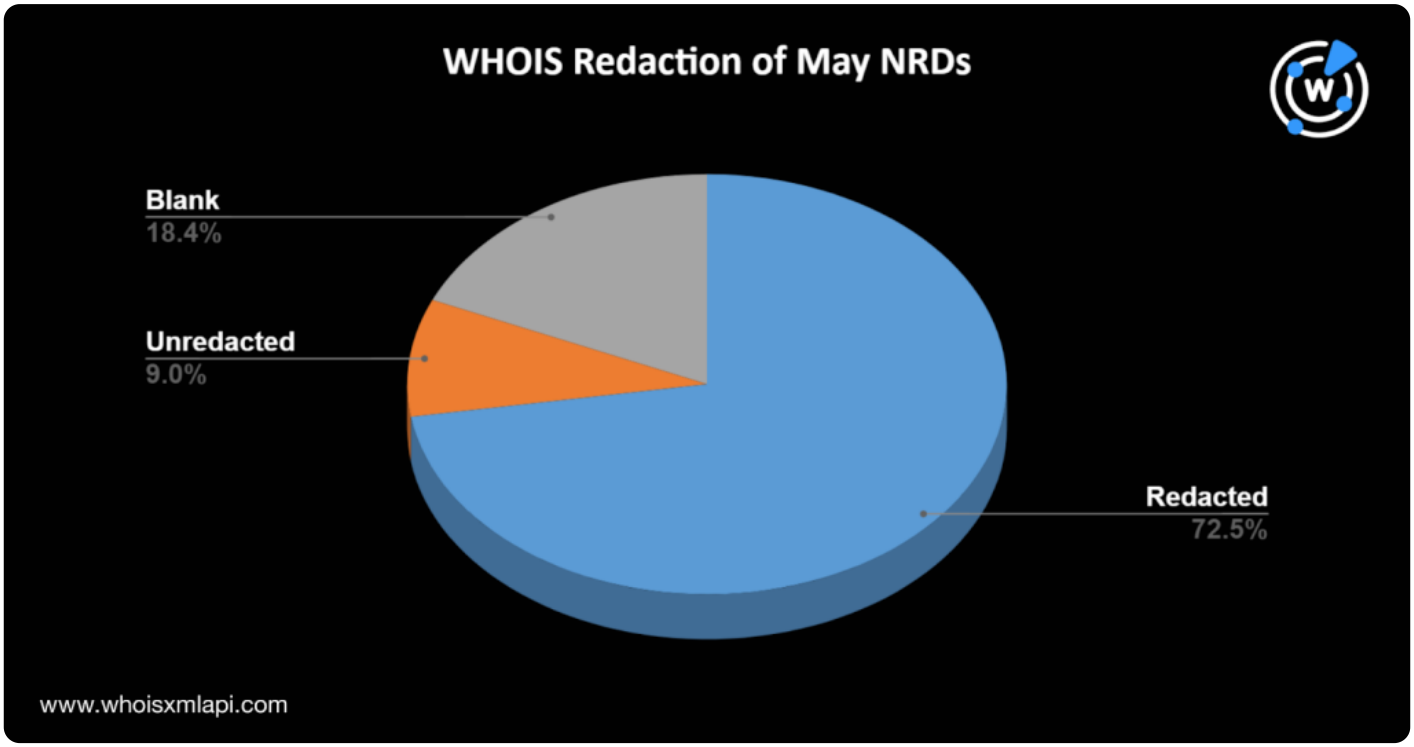
WHOIS 数据编辑

约有73%的新注册域名编辑过其WHOIS信息，大部分机构使用Domains By Proxy LLC的隐私编辑服务，占比约为29%。紧随其后的是Withheld for Privacy 和 Contact Privacy，占比分布为16%和12%。剩余排名前十的隐私保护服务提供商为Privacy Protect（占比5%），Whois Privacy Protection Service by onamae.com（占比4%），PrivacyGuardian.org （占比1%），Private by Design, LLC （占比1%），以及Whois Proxy（占比1%）。

一些注册人在其“注册机构”一栏填写“因隐私编辑”（占比2%）和“GDPR要求”（1%）。

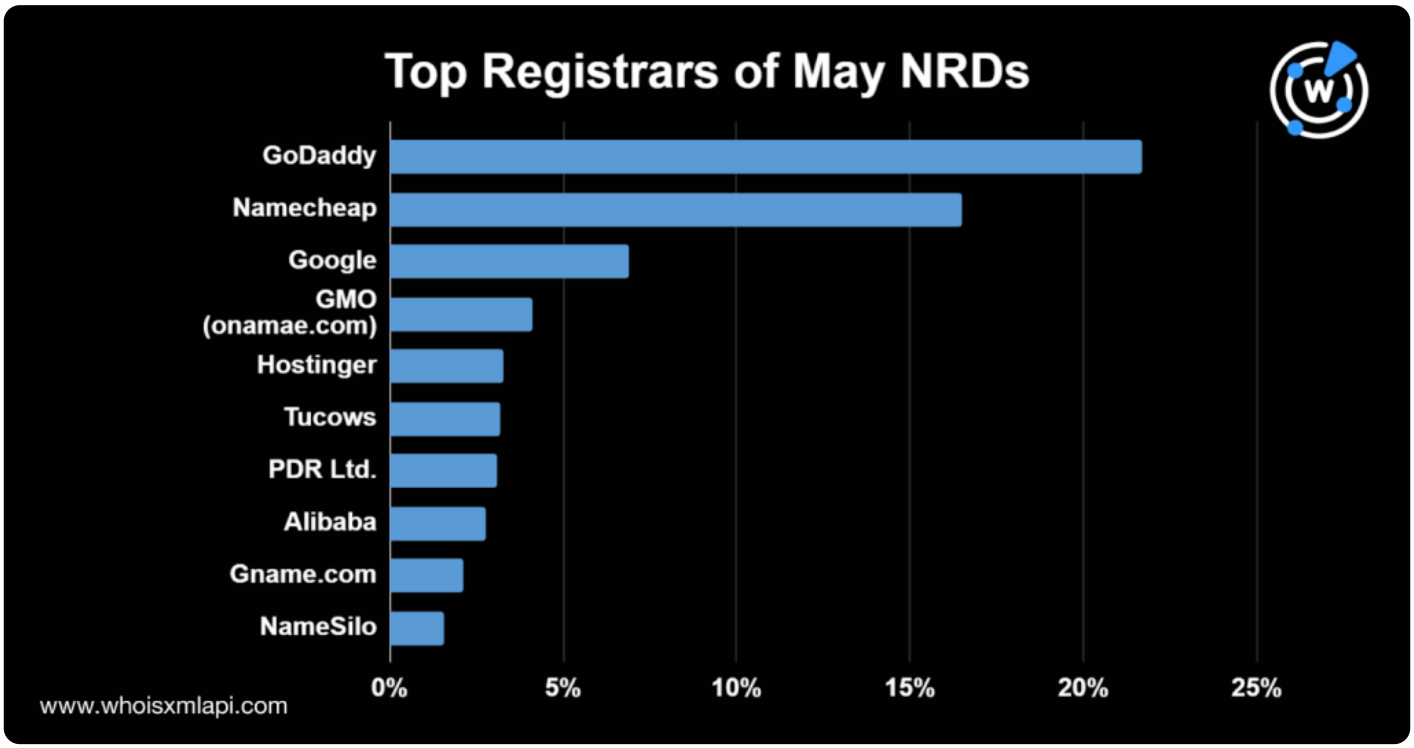


只有9%的新注册域名未编辑过其WHOIS信息记录，极少的机构公开了其注册的电子邮件地址。约有18%的



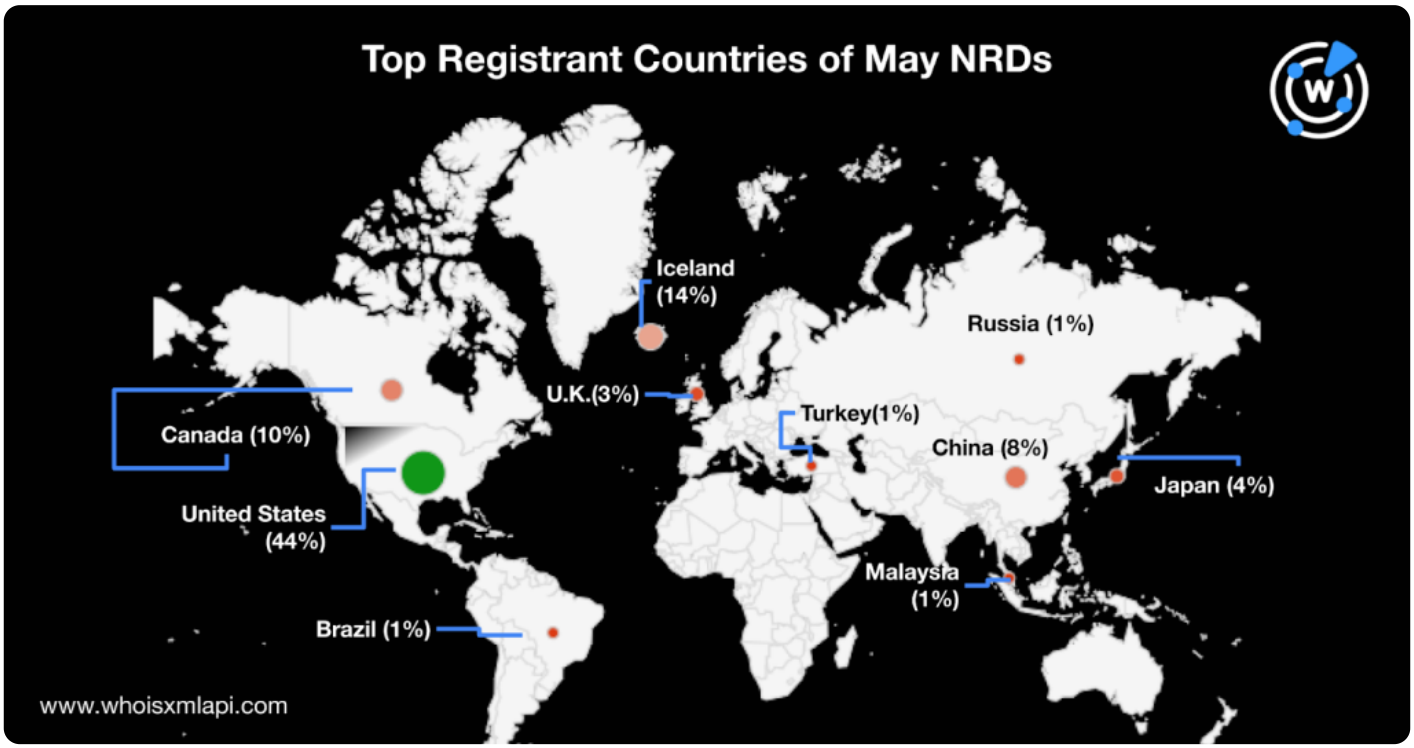
注册商分布

与2023年3月和4月相同，5月份GoDaddy依旧是排名第一的注册商，占域名注册总量的22%。剩余排名前十
GMO Internet占比4%，Hostinger 占比3%，UAB占比3%，Tucows占比3%， PDR
Ltd占比3%，阿里巴巴占比3%， Gname.com占比2%，以及NameSilo占比2%。



排名领先的注册国家

五月份新增注册域名中有44%的域名是在美国注册的，冰岛和加拿大注册的数量分别为14%和10%，中国注



二级域名中常见的字符串

国际化域名（IDNs）持续热门，Xn仍然是这几个月来最常用的文本字符串之一。此外，科技术语如ai、it和字符串job、bet和live也值得关注。具体详见下图词云。

从DNS角度透视本月网络安全问题

以下是我们5月份所发布的相关威胁报告。

- **利用DNS对苹果IOS14零点击间谍软件KingsPawn进行窥探：** WhoisXML API研究人员对KingsPawn相关联的域名进行详细的DNS搜寻，KingsPawn是一款仿照NSO集团的Peg
- **当营销供应商受到攻击，客户必然受到影响：** 揭露DNS中的第三方风险。在AT&T因针对其营销供应商的安全事件而遭受数据泄露后，我们的研究人
- **在DNS中追踪Bumblebee恶意软件的搜索引擎投毒的痕迹：** WhoisXML API研究人员对Bumblebee搜索引擎投毒攻击的妥协指标进行了列表分析，查找此处1900多个潜在的
- **DNS深度探究：VPN服务可能是由OpcJacker虚假伪装而成：** 我们的研究人员对OpcJacker进行了深度探查，这是一款数据窃取恶意软件，且伪装成一款VPN服务
- **在DNS中对内华达勒索软件进行数字碎片的搜寻** ：我们的研究团队调查并扩大了与内华达州勒索软件相关的IoCs列表，发现了一个可能与之相关的电

您可点击此链接查找更多报告内容。

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