2023年3月域名事件重点回顾

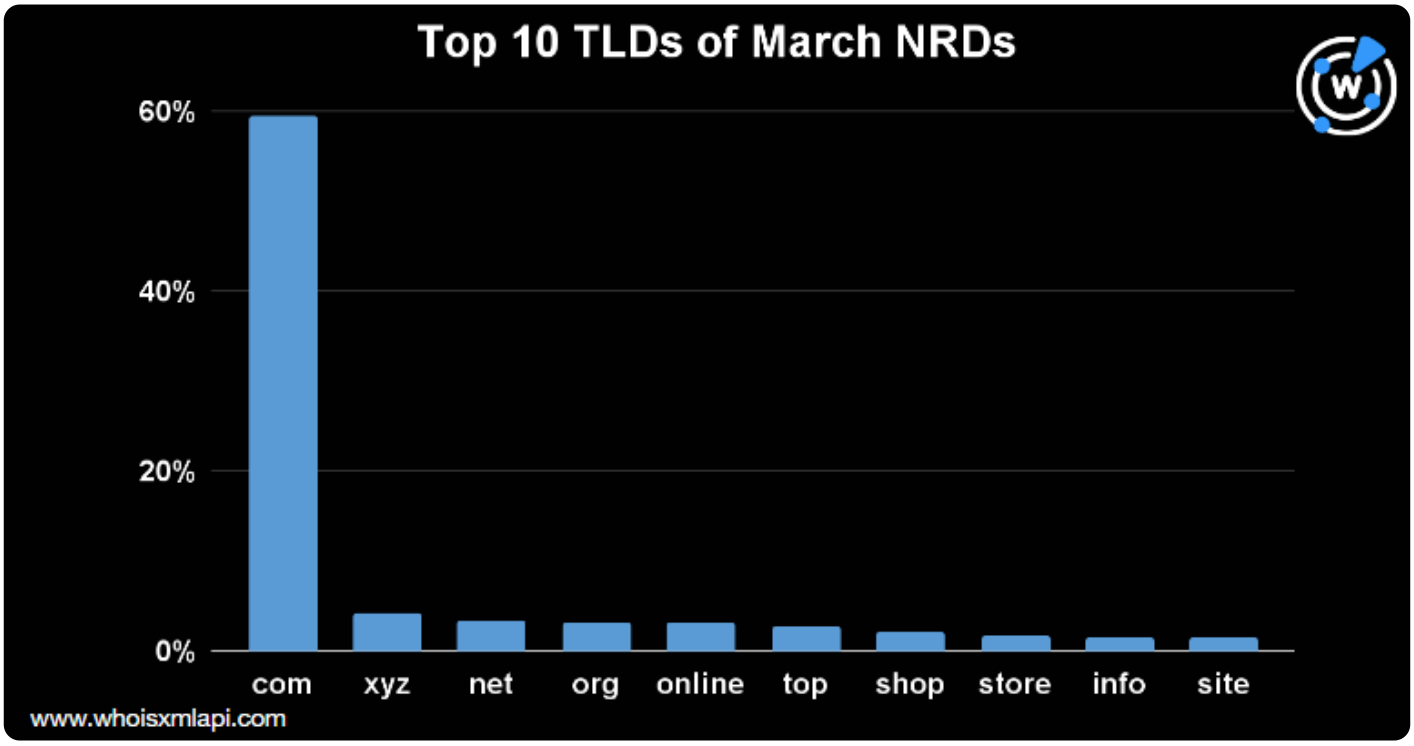
发布于 April 14, 2023

2023年3月1日-31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

3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3月份域名注册总量的60%，紧随其后的是.xyz（占比4%），.c



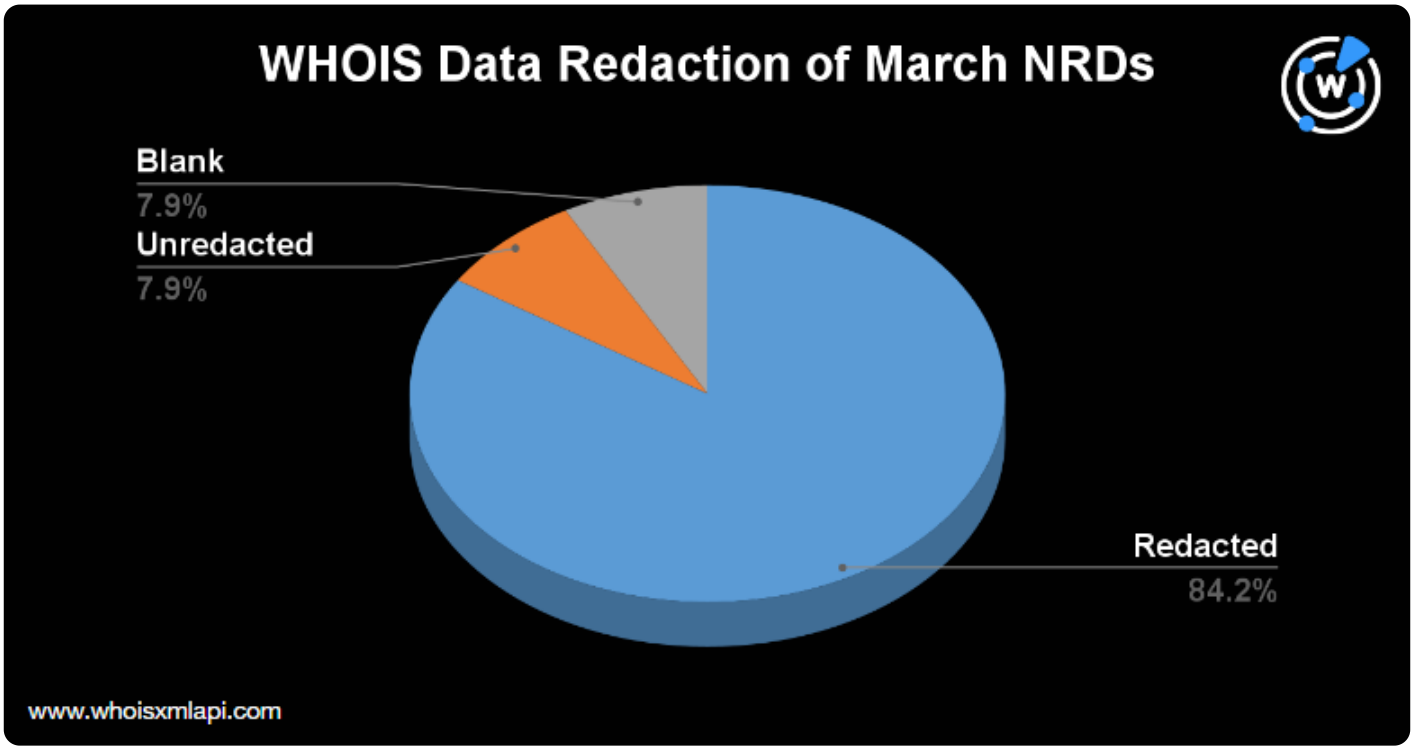
根据Infoblox在其2022年第四季度网络威胁报告中所列举出的最具风险的顶级域名，在三月份的新增注册域

通用顶级域	域名注册量占比3月份NRD注册总量
xyz	4.227%
top	2.855%
buzz	0.777%
click	0.723%
live	0.579%

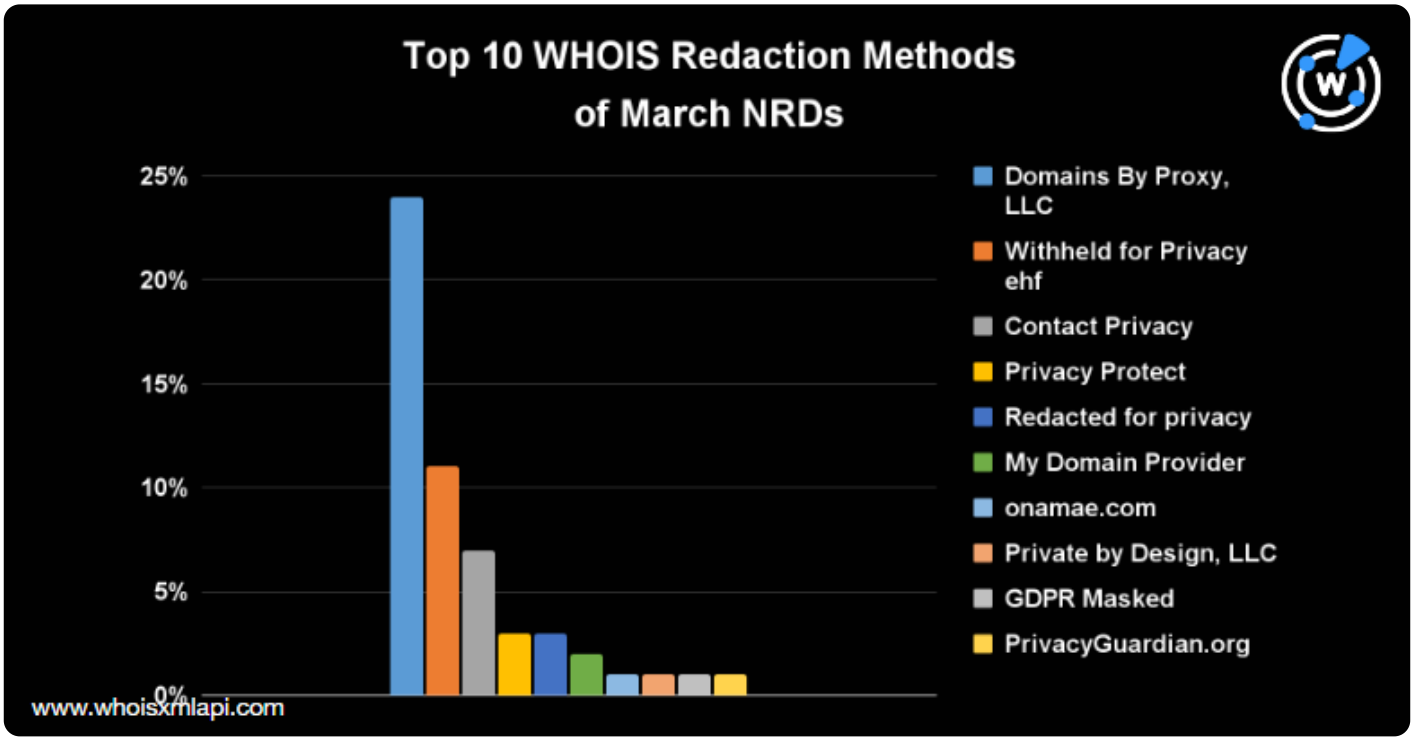
联系我们可获取完整列表信息。

WHOIS 数据编辑

三月份新注册的域名中只有8%的域名公开了相关的注册人信息，大部分域名进行了WHOIS数据编辑。



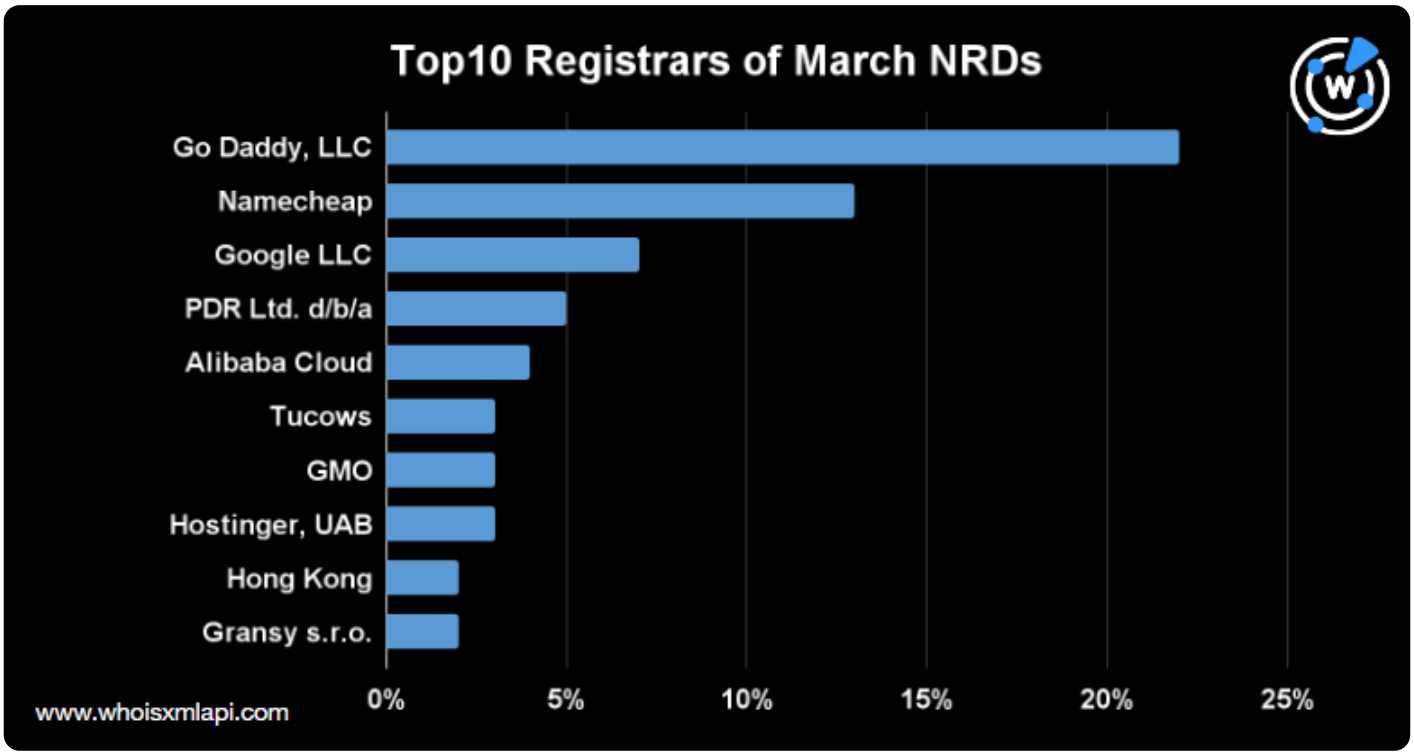
大约84%的域名根据其注册机构领域的不同，使用了隐私保护服务。在统计了使用WHOIS隐私保护服务和数
By Proxy （占比24%），Withheld for Privacy EHF (占比11%); Contact Privacy, Inc. (占比7%);
以及Privacy Protect LLC (占比3%)。下表则是最常用的排名前十的数据编辑服务提供商。



注册商分布

和1月和2月一样，GoDaddy排名注册商首位，占域名注册总量的22%，排名第二的注册商为Namecheap，
Ltd.，份额分别为7%和5%。

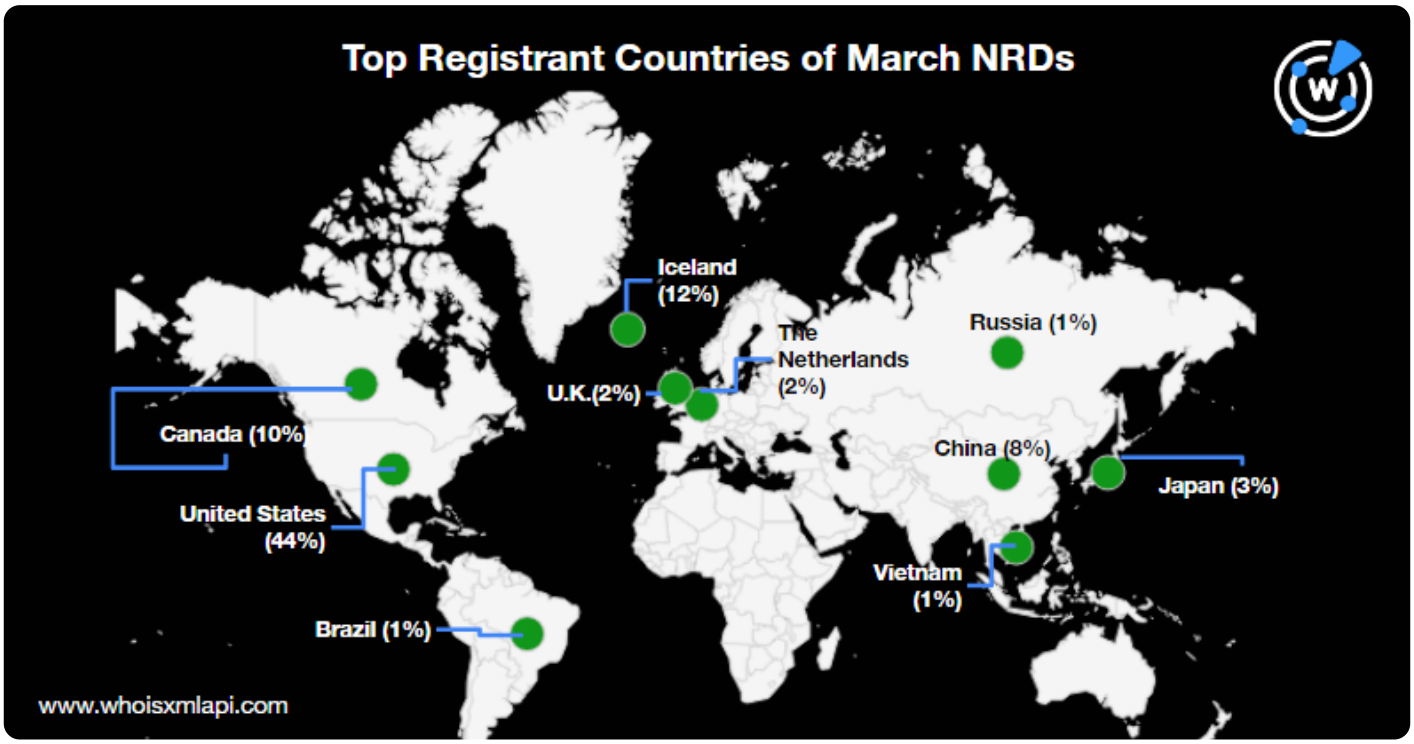
排名前十的注册商还包括阿里巴巴（4%）、Tucows（3%）、GMO（3%）、Hostinger（3%）、香港聚名
S.R.O.（2%），以及Gransy S.R.O.(2%)。详情如下表。



前十名注册商的域名数量占总域名注册量的63%，其余的域名则分布在其他的350个注册商中。

排名领先的注册国家

三月份新注册域名中有44%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%。其他注

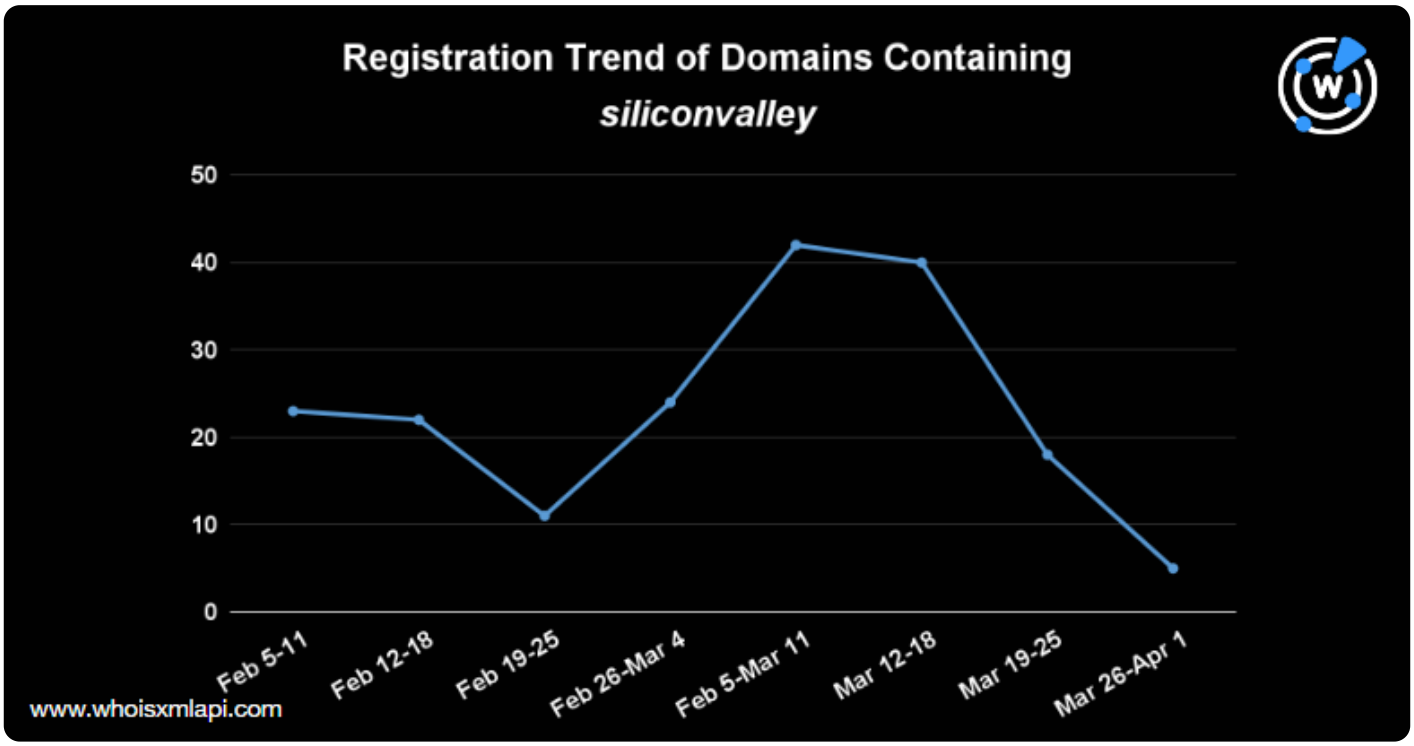


二级域名中常见的字符串

Xn仍然是这几个月来最常见的文本字符串之一，国际化域名（IDNs）也持续热门。此外，字符串如online、其他的使用频繁的科技类的术语包括ai、digital、app和web。常见的字符串详见下图词云。

新闻事件

3月份最重要的事件就是硅谷银行的动荡。DNS是如何反映这一事件？下表是事件概览图，显示了硅谷银行



从DNS角度透视本月网络安全问题

以下是我们3月份所发布的相关威胁报告。

- **通过DNS透视Lorec53网络钓鱼**：WhoisXML API研究人员扩展分析了Lorec53 APT集团在网络钓鱼和恶意软件活动中可能使用的妥协指标，发现了1800多个额外的相关域名。
- **你的内网容易受到攻击吗？调查DNS中的内网冒充行为**：在最近发生的Reddit安全事件中，攻击者模仿了该平台的内网网关，我们研究了DNS中的内网假冒行
- **用WHOIS和DNS照向国际欺诈行为**：对在线诈骗中使用的电子邮件地址的IoC进行详细分析后，我们发现了3000多个相关的域名。
- **医疗保健相关的IoCs：威胁扩展和HER仿冒探测分析**：我们分析了针对医疗机构的威胁行为之一，在对古巴勒索软件IoCs的调查分析后发现了数以千计的域

您可点击此链接查找更多报告内容。

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