2023年2月域名事件重点回顾

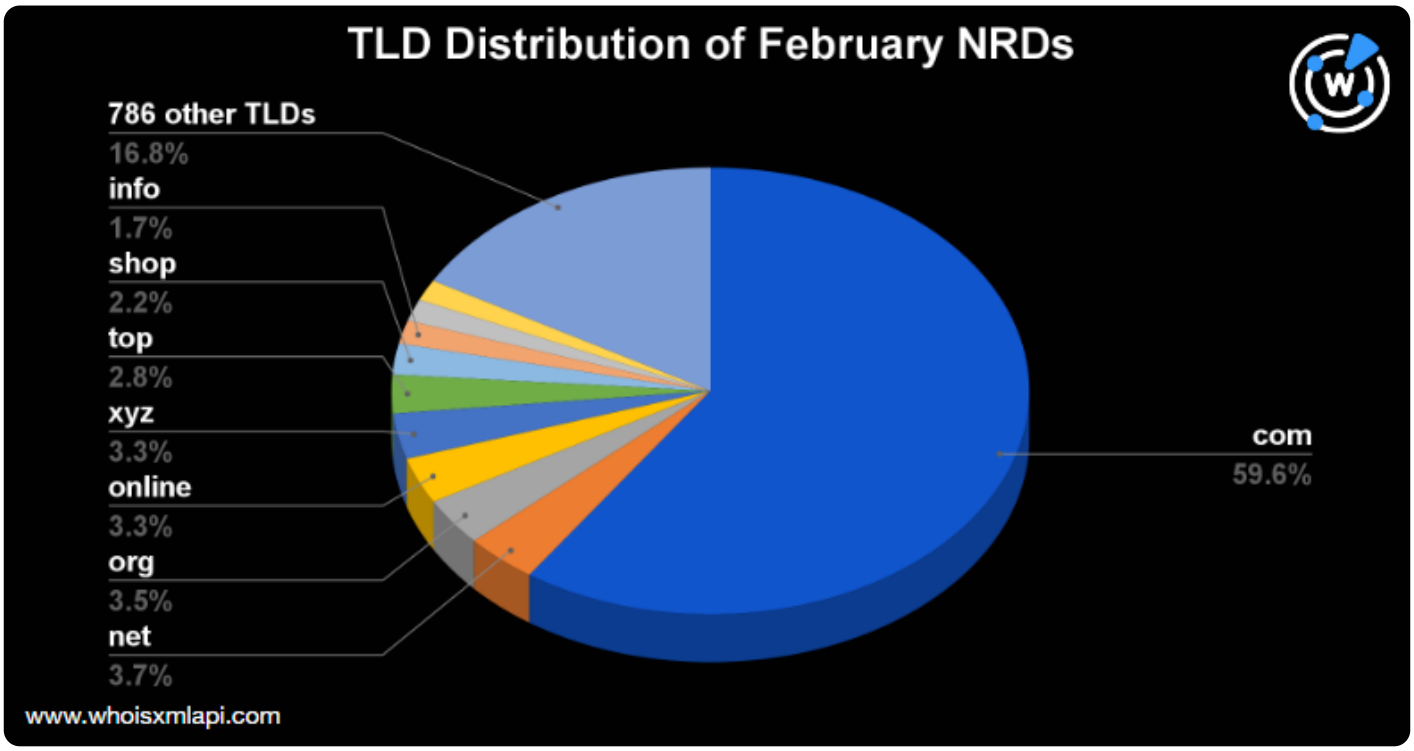
发布于 March 22, 2023

2023年2月1日至28日期间域名注册量约数百万，WhoisXML
API分析师从中随机选取了28,000个域名作为样本进行分析，研究这些域名的顶级域、注册商以及注册国家

2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2月份域名注册总量的59.6%，紧随其后的是.net（3.7%），.o



滥用最多的顶级域名的域名注册量

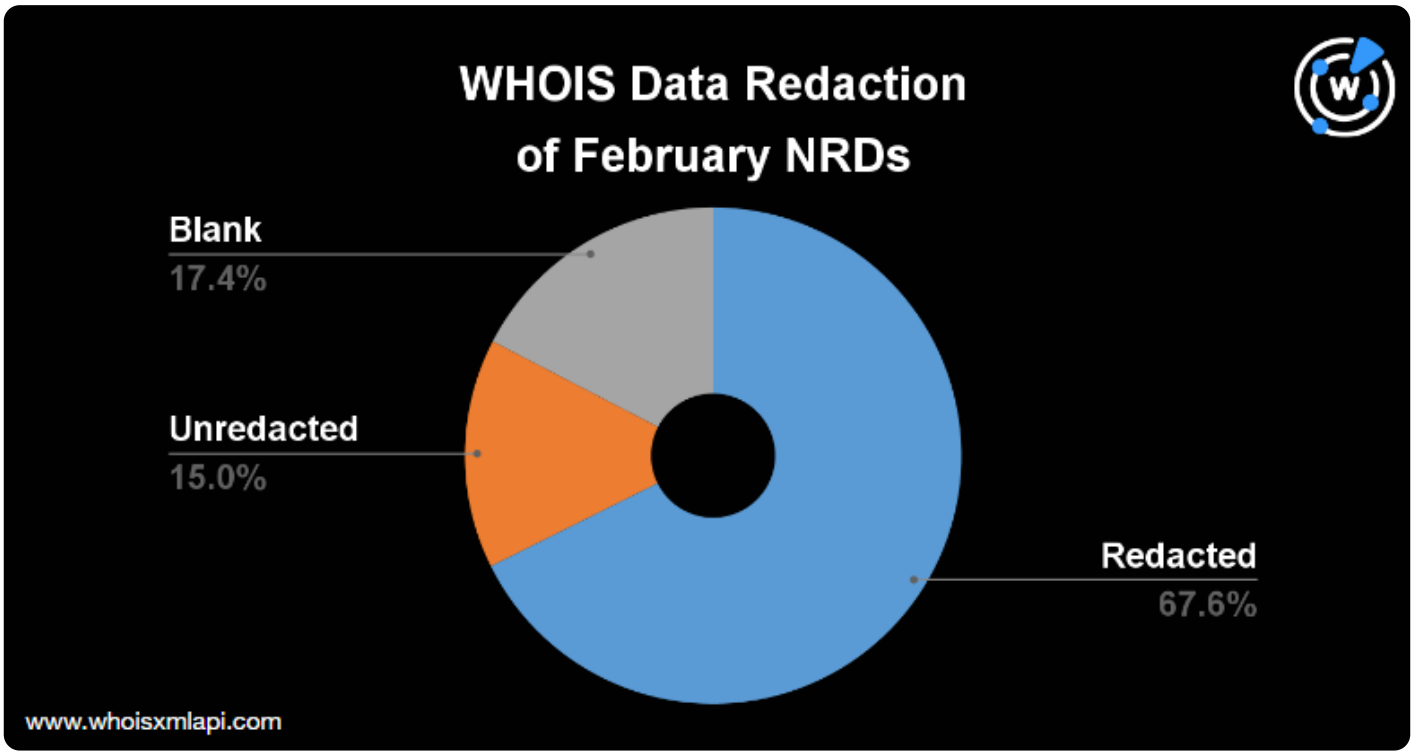
根据Spamhaus所提供的截止到2023年3月3日最滥用的顶级域名数据信息，我们重点关注了这些滥用域名的

顶级域名	滥用域名占Spamhaus所分析的域名总数的百分比	域名注册量占比2月份新增注册域名的总量
.live	31.0%	0.542%
.beauty	25.1%	0.076%
.fyi	21.0%	0.063%
.fit	24.7%	0.029%
.zone	28.5%	0.015%
.bar	27.6%	0.012%
.rest	71.7%	0.005%
.okinawa	69.6%	0.001%

尽管域名注册量占每种顶级域的数量低于1%，但是依旧需要重点关注这些域名，2023年2月间有数百万新增

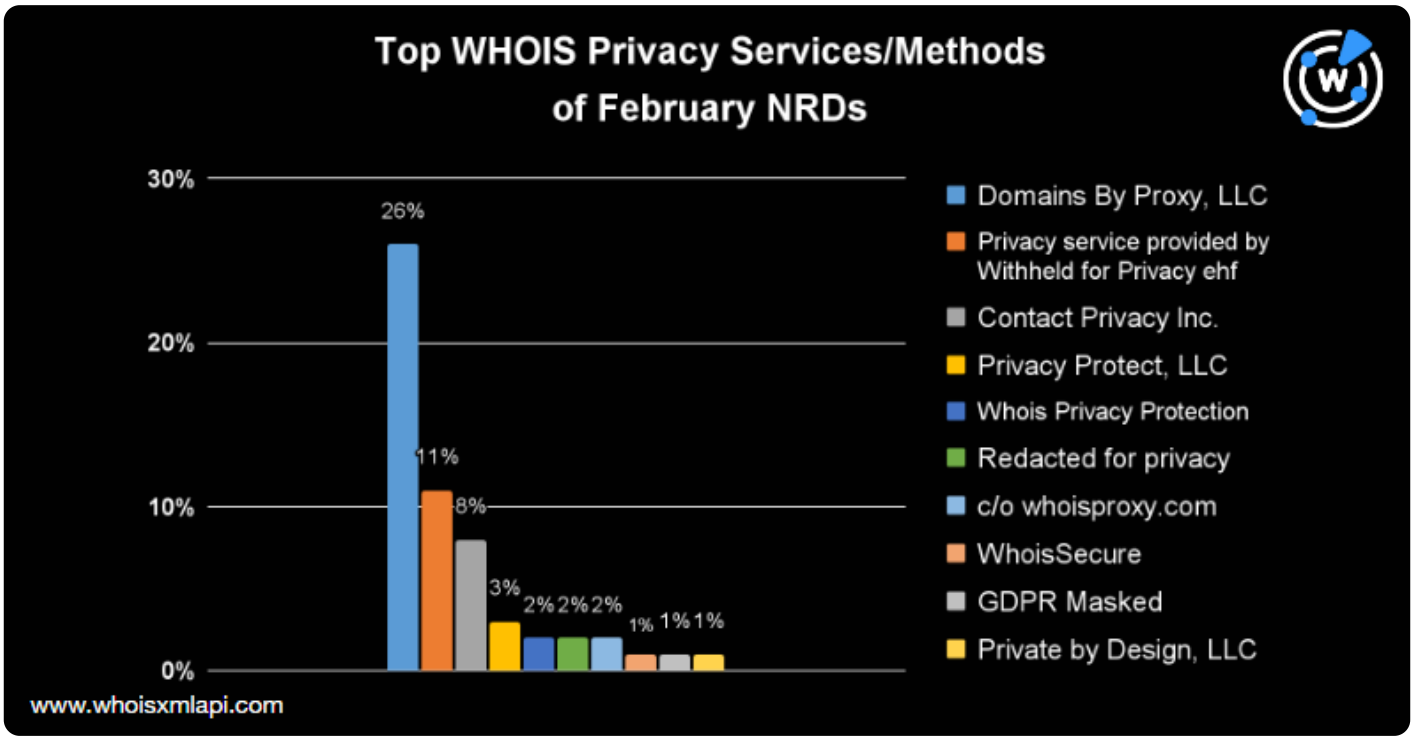
WHOIS 数据编辑

WHOIS数据编辑已经在全球范围内大规模推行了数年，对于2月份新注册域名而言也不例外。只有15%的域



大约67%的域名根据其注册机构领域的不同，使用了隐私保护服务。我们统计了排名前列的WHOIS隐私保护
By Proxy, LLC使用的最多，为2月份新增注册域名中1/4以上的域名提供了保护服务。

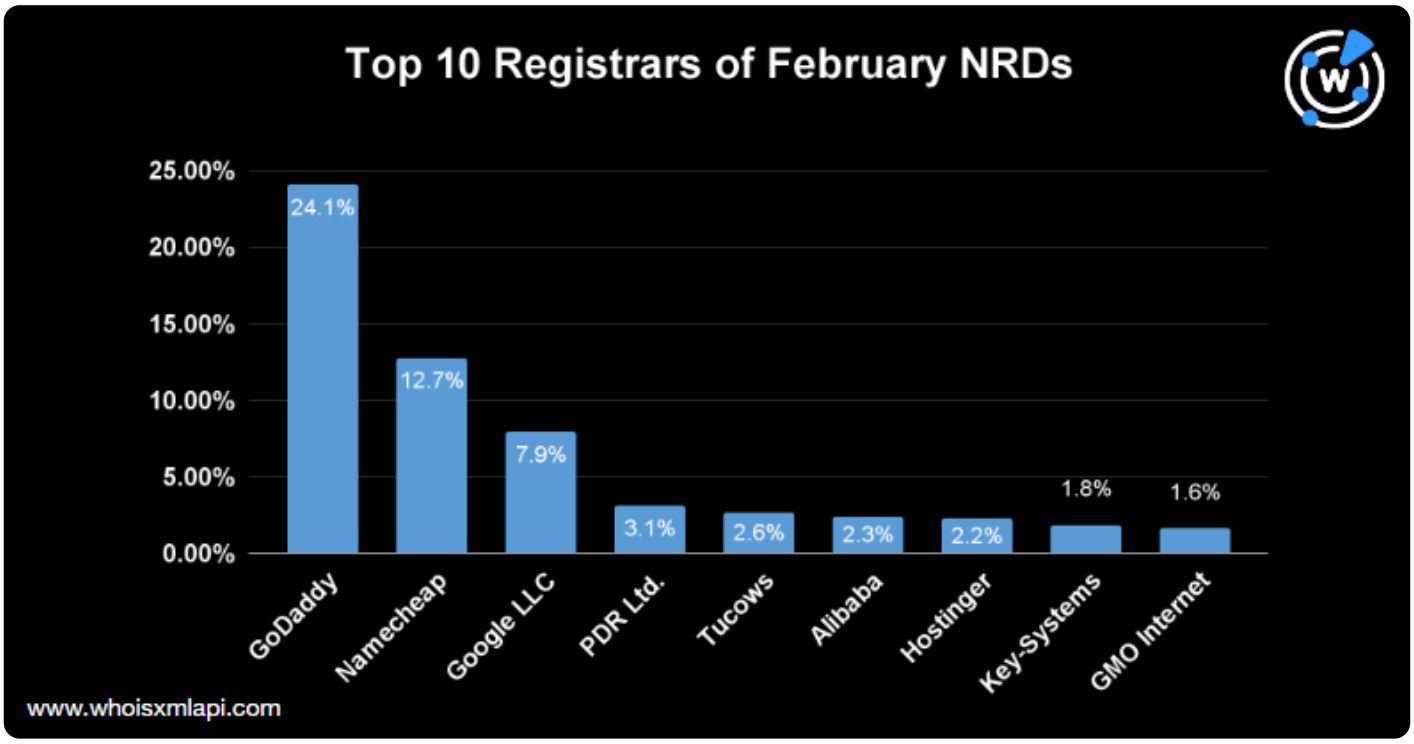
紧随其后的是Withheld for Privacy ehf，占比11%，以及Contact Privacy,
Inc.占比8%。在新注册域名的注册人机构栏中出现的其他编辑方式或字符串为Privacy Protect,
LLC，Whois隐私保护服务onamae.com，编辑隐私保护c/o
whoisproxy.com，WhoisSecure,GDPR Masked以及Private by Design, LLC。详情请见下图。



注册商分布

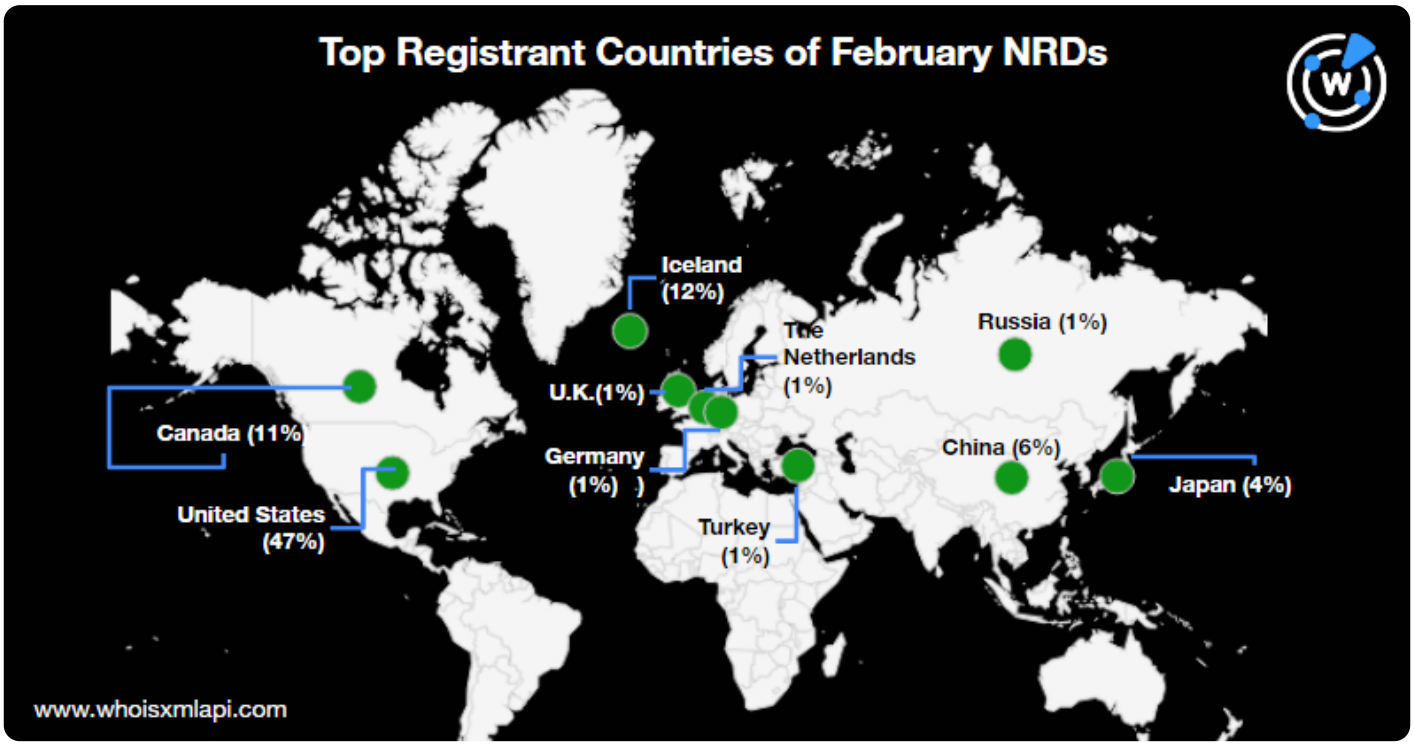
GoDaddy继续占据了域名注册量的较大份额，约为24%。Namecheap紧随其后，份额约为12.7%，谷歌为Ltd.为3.1%，Tucows为 2.6%, 阿里巴巴为2.3%，Hostinger 为2.2%，Key-Systems为1.8%，以及GMO Internet为1.6%。

总体来讲，排名前十的注册商占据了2月份新注册半数以上的域名，剩下的域名则分布在409家注册商中。



排名领先的注册国家

2月份几乎有一半的新注册域名是在美国注册的，而12%和11%的域名分别在冰岛和加拿大注册。其他注册



二级域名中常见的字符串

常用的互联网术语在新注册域名中依然很常见，包括***online***, ***shop***, ***market***, ***info***, ***tech***, 和***app***。同时，还有频繁出现的词AI。

国际化域名（IDNs）持续热门，可从XN的频繁使用中体现出来。2月份常见的字符串可详见下图词云。

从DNS角度透视本月网络安全问题

以下是我们2月份所发布的相关威胁报告。

- 对抗Hive勒索软件的斗争可能还没结束—未经确认的域名显示：我们的研究人员在对Hive勒索软件集团活动中所使用的6个妥协指标（IoCs）进行进一步扩展分析后
- 对已知的网络圣战IoC列表进行扩展分析：WhoisXML API威胁报告分析师Dancho Danchev最近发现了6个与网络圣战分子相关的电子邮件地址，这些IoCs直接指向了2200多个相关的
- 通过威胁矢量识别捕捉伪装成合法工具的Batloader：以17个确定为Batloader妥协指标的域名作为分析起点，我们发现了5000多个有一定关联性的其他
- 通过对IoC列表的扩展分析，衡量恶意软件Gigabud RAT的危害性：我们对Gigabud RAT的10个IoCs进行扩展分析，查找到了1000多个相关的数据信息，其中有数百个域名中含有机构的 de Comercio, Advice, Thai Lion Air, Shopee Thailand, SUNAT, 以及Kasikornbank。
- 追踪探索谷歌搜索广告与恶意软件传播间的关联性

：我们的研究人员对近期的一项恶意活动进行了深入调查，该恶意活动主要针对寻找开源软件下载网站

您可点击此链接查找更多报告内容。

??