

PassiveDNS 🔖 **Featured**

DeepSeek 出现大批仿冒域名并在持续增加中



zhangzaifeng

2025年2月3日 • 7 min read



注册时间分布如下:

注册商的情况如下:

在TLD方面

在注册人方面

在解析结果方面

域名用途

钓鱼欺诈类,用来窃取用户登录凭证或者诱骗用户购买相关的虚拟资产

域名抢注,以期后续能够通过域名获得较好的收益:

做AI研究相关的,通过这种方式提高其网站曝光度和紧跟研究热点

在网络安全领域，由于大规模的基础数据支持，奇安信Xlab在多个领域拥有很好的全局视野，能够实时监测互联网中的各种活动，也因此能够发现许多有趣的现象。每当出现重大突发事件或现象级的爆火产品，总会有不同目的的行为随之而来。我们不仅能看到技术进步如何推动社会发展，同时也能看到一些别有用心行为在暗中滋生。

例如，最近的加州大火引发了全球的关注，人们纷纷捐款以支援灾区。然而，黑客们却利用这种同情心，迅速设立假冒救灾网站，通过钓鱼手段骗取善款，导致不少善良的捐助者上当受骗。参见[这里的新闻报告](#)。

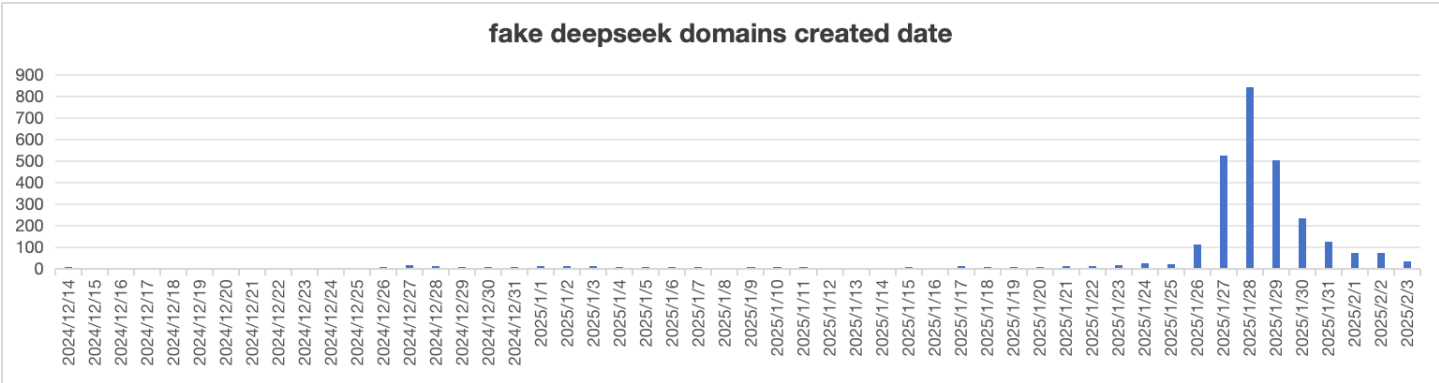
类似的情况，在科技领域的现象级事件中也屡见不鲜。最近，中国的DeepSeek 成为了人工智能领域的现象级爆火服务，短时间内吸引了大量关注。然而，我们在大规模域名观测系统中发现，DeepSeek 的爆火也带来了大量的仿冒网站、钓鱼网站。目前，我们检测到的仿冒 DeepSeek 相关网站数量，已成为近期监测数据中仿冒、抢注、钓鱼最多的类别之一。**通常假冒抢注的网址数字多在十位级别至多百级别，但是这次，我们已经看到了超过2千个域名，而且现在看这个数字还在快速增加。**

这类模仿现象，有的可能只是出于商业目的，想借助 DeepSeek 的热度售卖有前途的域名或者吸引用户；但也有不少恶意行为者，利用相似的域名和界面来误导用户，甚至传播恶意软件、窃取个人信息或骗取订阅费用。除此之外，我们还看到骗子紧跟技术潮流，利用市场的兴奋情绪，推出所谓‘DeepSeek 加持’的各种高大上功能的空气币（无实质价值的虚拟货币），甚至出现所谓购买deepseek内部原始股的网站。这种模式与过往许多科技爆款（如 ChatGPT）在爆火后迅速出现大量仿冒和诈骗的趋势高度相似。可参考[cyble的相关分析](#)。

因此，我们统计了从2024年12月01日到2025年2月3日两个月的时间域名注册情况，共观察到**2650**个仿冒deepseek的网站。首次看到仿冒deepseek域名的注册时间在2024.12.14，绝大多数的域名注册在2025.1.26之后。此外由于数据获取有一定的延迟，因此真实数字要比这个数据会更大。

注册时间分布如下：

大规模的仿冒注册从1.26开始，1.28达到顶峰，超过800个域名，随后几天数据有所下降。



注册商的情况如下：

- 1. 共涉及180个左右不同的注册商
- 2. Top10的注册商占了总域名数量的69%
- 3. 同正常域名注册类似，头部的几个分别为GoDaddy，阿里云以及 Spaceship等域名注册商。

在TLD方面

最多的仍然是通用顶级域， 其次是国家顶级域以及新顶级域。

TLD的具体分布如下：

在注册人方面

绝大多数的域名注册人都采用了隐私保护。无法看出是否存在同一个实体进行大量注册的情况。

在解析结果方面

美国有全球最大的域名注册机构和云服务商，所以解析结果60%位于美国。接下来是新加坡，德国，立陶宛，俄罗斯和中国。这六个国家占了总解析IP数量的86.9%。

从AS来看，主要解析在域名注册商和云服务厂商中。

从域名解析结果来看，这些域名的使用主要有如下几个用途：

钓鱼欺诈类，用来窃取用户登录凭证或者诱骗用户购买相关的虚拟资产

钓鱼相关页面如下：

通过空气币诱骗用户的网站有很多，列举几个如下：

除了常规的空气币诈骗之外，骗子甚至宣称可以**抢先购买deepseek原始股**，着实很动心暴富的机会来。

域名抢注，以期后续能够通过域名获得较好的收益：

比如下面这种deepseekagent.com目前标价37.95万人民币，即使deepseek目前的热度，这个价格也已经着实不低了。

做**AI**研究相关的，通过这种方式提高其网站曝光度和紧跟研究热点
比如下面的站点：

一些域名样例

deepseekr3.com

deepseekwin.com

deepseekcto.com

netdeepseek.com

deepseekgod.com

domaindeepseek.com

deepseek-ai-assistant.com

localdeepseek.com

deepseekv3.com

deep-seek-r1.pw

seeksdeeper.com

deepseeky.com

deepseekai.pics

finetunedeepseek.com
deepseekjournal.com
ideepseekai.com
deepseek-chat.vip
discoverdeepseek.com
learndeepseek.org
deepseek.cam
deepseekportfolios.com
deepseeksol.xyz
deepseekmoscow.ru
deepseeknow.xyz
godeepseek.xyz
deepseekspan.com
agideepseek.com
deepseekworkflow.com
openaideepseek.com
deepseek-ai.space
bdeepseek.com
deepseekaiapk.com
deepseek-bank.com
deepseek27.com
deepseekindustry.com
deepseekcoin.net
deepseekpartners.org
aideepseek.se
deepseekasia.online
8deepseek.com
deepseekphone.com
deepseek123.com

受影响情况及安全建议


从我们PassiveDNS数据来评估，这些域名的流行度都不太高。绝大多数的域名访问量都极少，只有3个域名的访问来源数量超过50。


尽管这些伪造的deepseek域名在应用形态方面呈现出多种形式，不过这些域名的解析都处在快速的变化之中。


出于严格的安全考虑，建议用户在访问deepseek相关的服务时，务必访问其官方网站deepseek.com 以及 deepseek.cn。其他的域名除非你能够确认访问的身份，否则不建议进行深度交互，尤其是涉及到用户名密码相关的敏感数据，都需要慎之又慎。


What do you think?


0 Responses


Upvote

Funny

Love

Surprised

Angry

Sad

0 Comments

Login

G

Start the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS

Name

Share

BestNewestOldest

