

关于中国境外自治域 AS 402425 恶意篡改部分 DNS 解析数据的调查报告

近期，中国多个省份多次发生用户访问请求异常跳转至博彩网站的事件，对广大人民的财产安全和正常上网权利造成了严重危害。经分析，攻击者利用中国境外自治域 AS 402425，主要采取宣告虚假路由、篡改域名解析数据等手段进行攻击，危害范围广泛，特此公布有关调查情况，为全球相关国家、单位和广大网民有效发现和防范此类攻击提供借鉴。

一、网络攻击过程

（一）通过宣告虚假路由劫持流量。攻击者在互联网路由注册库注册虚假源地址前缀和虚假自治域集合，利用其控制的自治域发布虚假源地址前缀和虚假短路径，对中国境内部分流量进行劫持。

（二）篡改劫持流量中的 DNS 解析数据。攻击者劫持流量后，对其中的 DNS 解析数据进行篡改，主要有两种手法：一是将 DNS 解析值直接修改为博彩网站地址；二是将 DNS 解析值指向恶意 DNS 服务器地址，用户向恶意 DNS 服务器请求域名解析时会返回博彩网站地址。

二、网络攻击定位

通过技术测量，确认域名篡改发生在中国境外自治域 AS

402425 内。该自治域由美国公司 QOREXA LABS 于 2026 年 4 月 9 日在美洲互联网号码注册管理机构 ARIN 注册，该公司官网显示其经营比特币相关业务。

三、域名篡改后指向的部分恶意 IP 地址

序号	IP 地址	序号	IP 地址
1	112.121.185.110	11	112.121.185.234
2	112.121.185.186	12	112.121.185.98
3	112.121.185.202	13	117.55.193.146
4	112.121.185.206	14	117.55.193.154
5	112.121.184.110	15	43.230.161.215
6	112.121.184.230	16	43.230.161.159
7	112.121.185.22	17	43.230.161.166
8	112.121.185.210	18	43.230.161.165
9	112.121.185.214	19	43.230.161.213
10	112.121.185.230		

四、防范建议

建议全球相关国家、单位强化风险意识，及时开展排查处置，重点做好以下防范工作：

（1）地区互联网注册机构、IP 地址交易平台等互联网号码资源相关机构应及时核查并注销 AS 402425 等恶意 AS 资源。

（2）网络运营商应在边界路由设备配置路由过滤策略，对路由宣告进行校验，拒绝接收并删除包含 AS 402425 的恶

意路由。

(3)互联网平台应加强监测核心业务域名解析 IP 变化、DNS 应答报文异常、路由路径异常变更等，及时发现劫持行为。一旦确认发生劫持事件，及时向上游运营商申告，要求处置异常路由宣告，切断劫持链路。

建议广大网民强化风险意识，加强安全防范，避免不必要的经济损失，具体包括：

(1) 使用经过验证的可信公共 DNS 服务，避免使用来源不明的 DNS 服务。

(2) 出现页面跳转恶意网站时，不要点击页面内任何按钮、链接，不要下载页面提供的程序，立刻关闭网页，并及时清理浏览器缓存。

(3) 保持终端操作系统、浏览器更新至最新版本，开启系统安全防护软件，防范跳转页面附带的恶意脚本、钓鱼等攻击。