Investigation Report on Malicious Tampering with Certain DNS Resolution Data by Overseas Autonomous System AS 402425 Outside China

Several provinces in China have recently experienced multiple incidents in which users' website requests were abnormally redirected to gambling websites, posing serious threats to the property security of the public and their right to access the Internet. Analysis has found that the attackers leveraged the overseas autonomous system AS 402425 located outside China to carry out attacks, primarily by announcing false routes and tampering with domain name resolution data. Given the extensive impact of these attacks, the findings of the attacks are hereby disclosed to provide a reference for relevant countries, organizations, and Internet users worldwide to effectively detect and prevent such attacks.

I. Attack Process

(1) Hijacking Traffic by Announcing False Routes. The attackers registered bogus source address prefixes and bogus autonomous system sets in Internet Routing Registries (IRRs). Using autonomous systems under their control, they announced false source address prefixes and short AS paths to hijack part of Chinese users' traffic.

(2) Tampering with DNS Resolution Data in Hijacked Traffic. After hijacking the traffic, the attackers tampered with the DNS resolution data therein, mainly through two methods: first, directly modifying DNS resolution values to addresses of gambling websites; second, redirecting the DNS resolution values to malicious DNS servers. When users request domain name resolution, the malicious DNS servers will return addresses

of gambling websites.

II. Attack Attribution

Technical analysis confirmed that the domain name tampering occurred within the overseas autonomous system AS 402425 outside China. The autonomous system was registered by a U.S. company QOREXA LABS through the American Registry for Internet Numbers (ARIN) on April 9, 2026. According to the company's official website, it operates Bitcoin-related business.

III. Subset of Malicious IPs Pointed to by Tempered Domain Name

No.	IP Address	No.	IP Address
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		

IV. Mitigation Recommendations

Countries and organizations worldwide are advised to strengthen risk awareness, and promptly conduct investigation and remediation, with a particular focus on the following preventive measures:

(1) Regional Internet Registries (RIRs), IP address trading platforms, and other entities related to internet number resources should promptly review and de-register malicious AS resources, including AS 402425.

(2) Internet service providers are advised to configure route filtering policies on border routers, validate route announcements, and reject and remove any malicious routes containing AS 402425.

(3) Internet platforms should strengthen monitoring of changes in the resolved IP addresses of core business domains, anomalies in DNS response packets, and abnormal changes in routing paths, so as to promptly detect hijacking activities. Once a hijacking incident is confirmed, they should immediately notify and request upstream service providers to address the anomalous route announcements and cut off the hijacking path.

Internet users are advised to strengthen their risk awareness and security precautions to avoid unnecessary financial loss. Specifically:

(1) Use trusted, verified public DNS services, and avoid using DNS services from unknown source.

(2) If a webpage is redirected to a malicious website, do not click any buttons or links on the page, or download any software from the page; close the webpage immediately, and clear the browser cache in a timely manner.

(3) Keep the endpoint operating system and browser updated to the latest versions, and enable security software to protect against malicious scripts, phishing, and other attacks delivered through redirected pages.