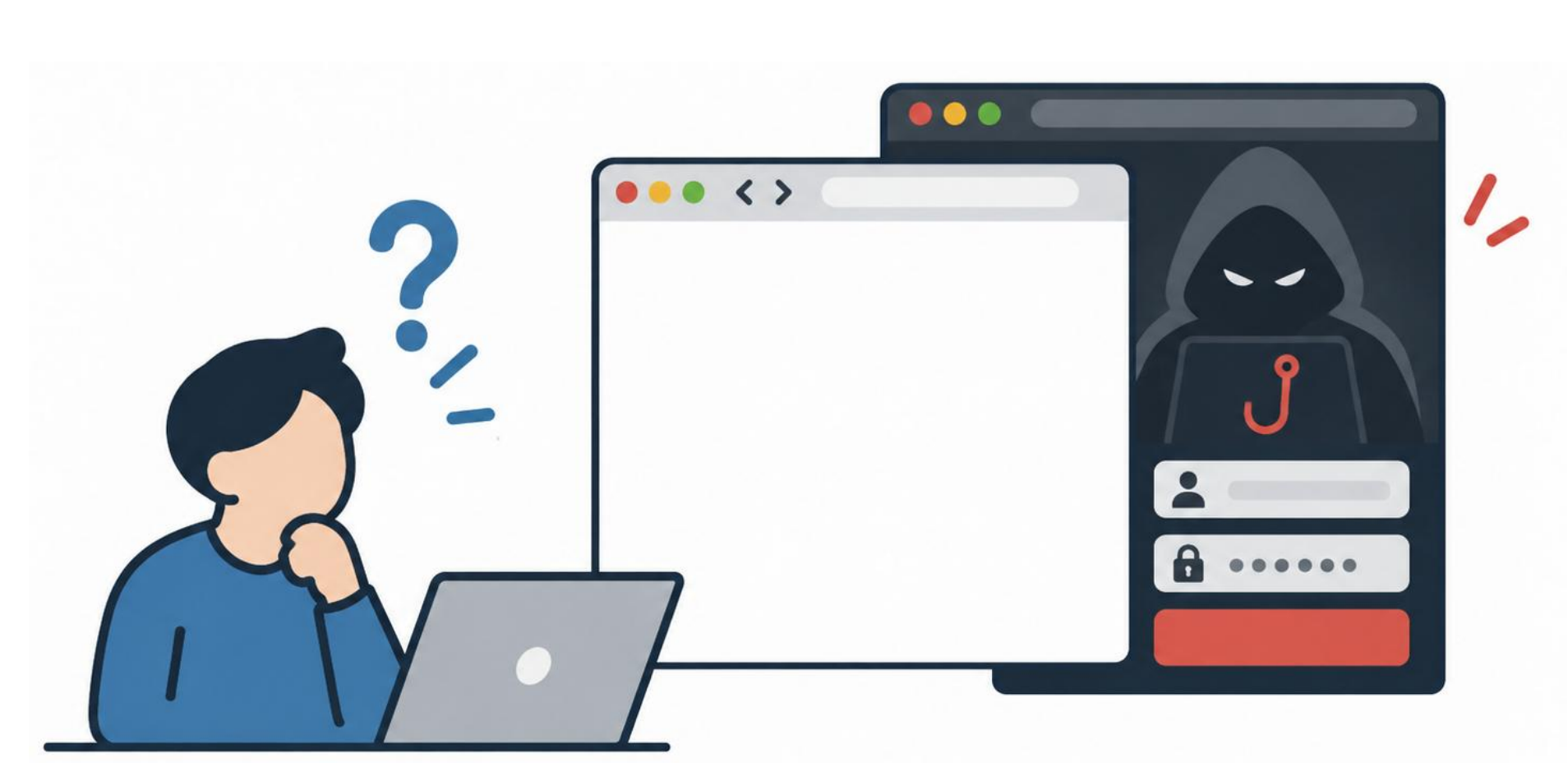


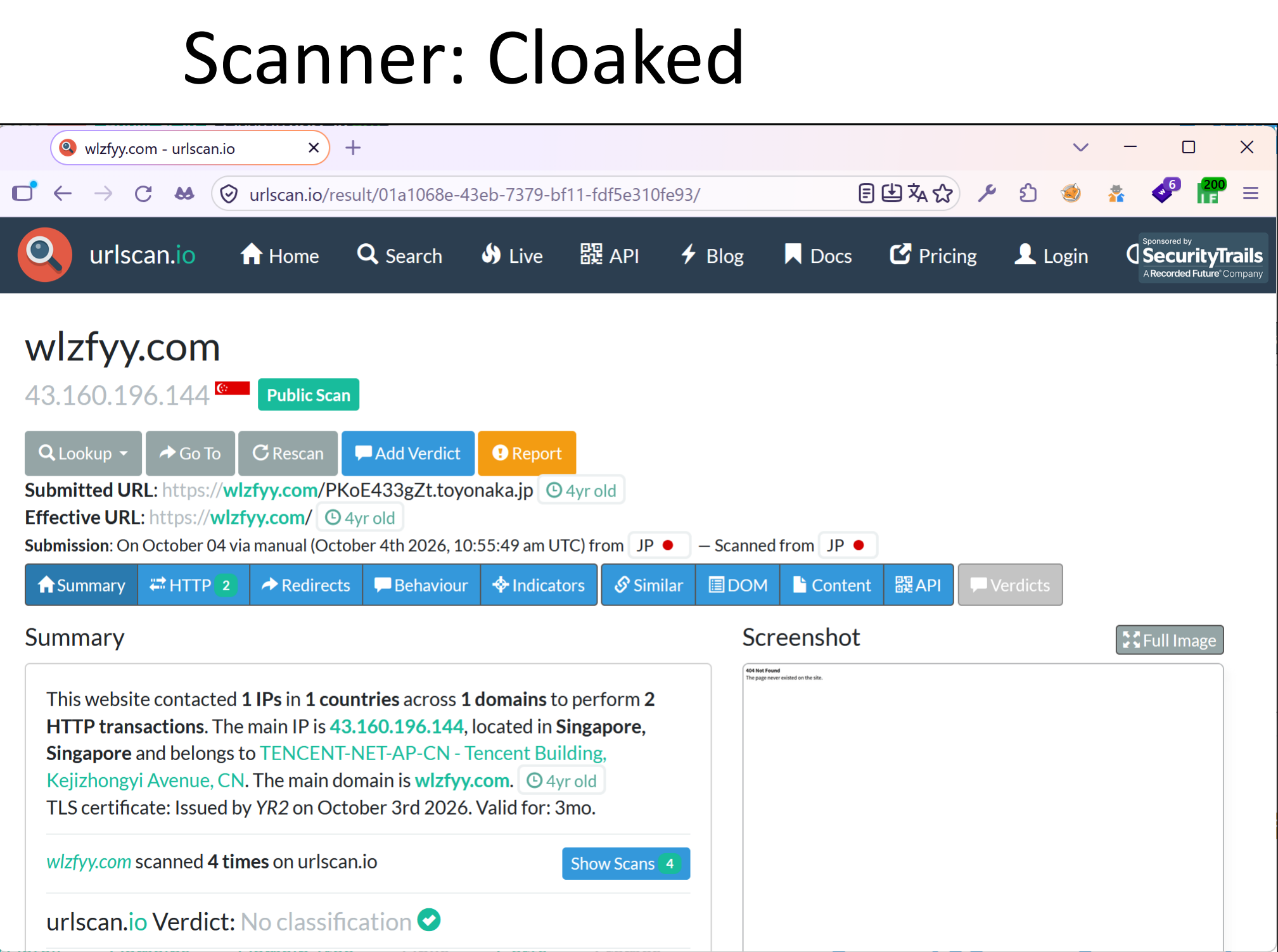
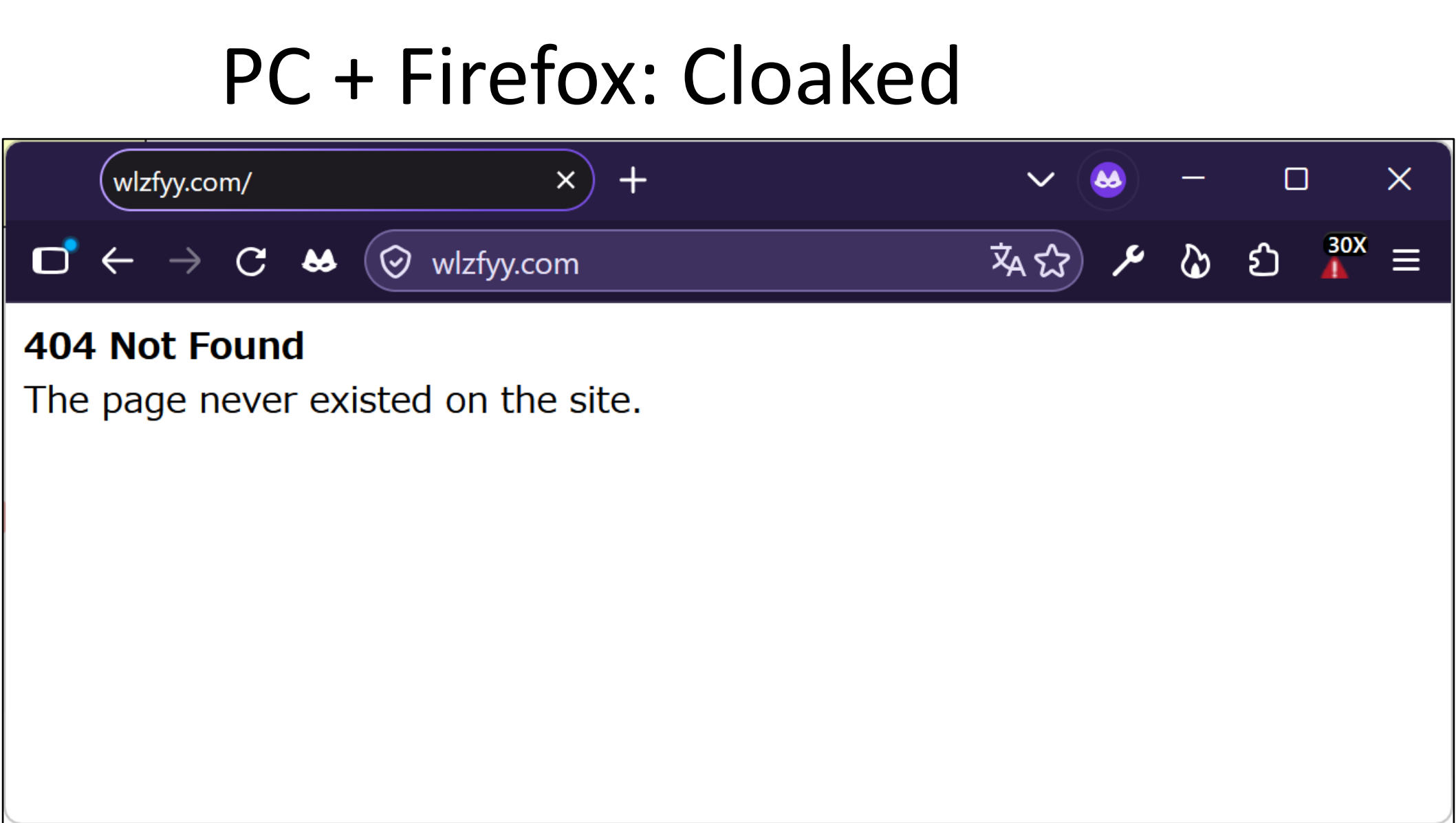
I’m struggling with phishing sites hidden by **cloaking**.



You Can’t Take Down What You Can’t See: The Growing Impact of Phishing **Cloaking**

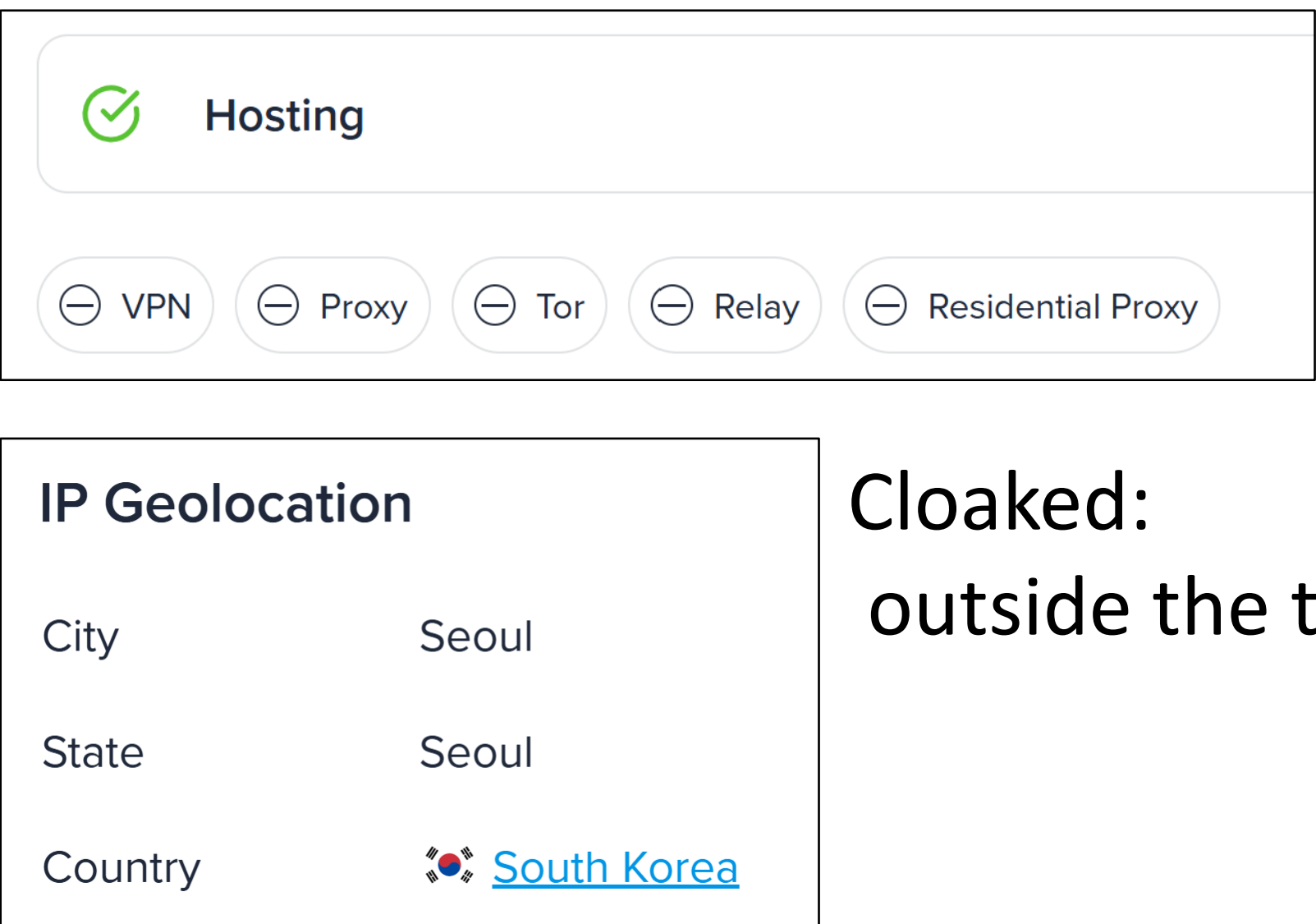
What is Cloaking?

- Phishing sites are shown only to intended victims
- Scanners and researchers see a benign, blank, or error page
- Typical Gating Conditions
 - Smartphone + mobile/residential IP + target geolocation



Attacker Cloaking Techniques

- Geofencing 🇯🇵
- User-Agent
- Accept-Language
- Headless browser detection
- Mobile/Residential IP
- Browser/Device Fingerprinting
- Redirect Tokens



Cloaked:
non-mobile / non-residential IP

Cloaked:
outside the target country (Japan)



Operational impact

- Costs and Delays...
- Safe Browsing warnings
 - Harder to automate scanning
 - Delayed or failed takedowns
 - Reduced visibility for researchers outside the target country

Are you facing the same problem?
What approaches have worked for you? Let’s discuss.

Contact

Osumi, Yusuke 大角 祐介
Sumitomo Mitsui Banking Corporation
Personal: ozuma5119@gmail.com
Work: osumi_yusuke@dn.smbc.co.jp
<https://about.me/ozuma>