Case study of P/P service abuse - GMO

One day in March 2018, when I was doing some open source research about Proxy/Privacy service, I happened to discover a P/P service provider’s email address - **proxy@whoisprotectservice.com**. According to open source tool ‘Viewdns.info’, there are **1,768,184** domains use the same email address in Whois record (screenshot as below).



If you search the same email address on Yumi – a Chinese domain trading company’s website, there are **1,195** newly registered domains use this email address in Whois record.



I randomly checked some of them, several of them linked to porn websites with Mandarin interface, and all of them hosted on same IP.

Then I conducted a reverse IP lookup to see how many domains are hosted on the same IP in total. The result is scary, **434,550** domains were hosted on the same IP at that time.



I checked the domains identified on Yumi for several days, the web content changed already, and most of the domains are now redirected to a static webpage as below.



The perception is that these domains were intentionally registered for malicious purpose, and served as bulletproof hosting. My previous working experience was that criminals will take advantage of the difference of applicable laws in different jurisdictions, to avoid detection of the police. This has been an open secret for years. For example, criminals will set up porn or online gambling websites which are hosted other than China, while the interface is in Mandarin, the administrator, moderators and the registered members are all from China.