Grace Jiang

Website analysis

My investigation focuses on a Chinese-based platform that distributes illegal pornographic content, including videos depicting sexual assault, voyeurism and drug-facilitated sexual assault. The platform regularly updates and changes domains to evade detection. Some videos contain victims’ personal information, including names and workplaces.

The website displays multiple alternative domains on its front page. At the bottom of each page and video, an email address ([91cg@pm.me](mailto:91cg@pm.me)) is provided for users to request the newest domain addresses if blocked. My initial investigation focused on tracing this contact point. I used Epieos, a tool recommended in Jon Keegan’s slides, to identify other services or platforms associated with this email address. This search yielded no results. To verify the validity of the email, I attempted to share a Google Doc with this address, which confirmed it was not a valid Google email account.

Shifting focus to the website’s domains, I noticed an unusual structure. When searching for the site via Google, users are first directed to a menu page hosting multiple domains before being redirected to the actual content. Using DomainTools, I analyzed what marked to be a permanent domain. The results showed a risk score of 1 (derived from proximity), first observed on September 27, 2022, at 12:30 PM, with an age of 908 days, and IP location in the United States (California, San Jose). The hosting history showed a change on December 6, 2024, with the post-action IP being 104.21.16.1. I conducted a follow-up search on this IP using DomainTools, though I’m still analyzing the significance of these results (there are many professional words I don’t understand, for example: Subject DN; Authority Key Identifier; Authority Info Access and so on, I also don’t know whether these are useful info).

I then investigated what I believe is the main current domain (<https://admit.pmfrwcdz.xyz/>). This analysis showed a risk score of 77, associated email [abuse@godaddy.com](mailto:abuse@godaddy.com) (connected to approximately 72,173,072 domains), and various registrar statuses including clientDeleteProhibited and serverTransferProhibited. I noticed a concerning age discrepancy: the domain is only 24 days old, yet contains videos dating back to February 14, 2022. The domain shares an IP address with three other domains: 91cg6.co, bitrzxcx.org, and bskibefs.com (all currently inaccessible), with an IP location in Hong Kong (Aberdeen - Stepgo Limited). Based on this information, I suspect the domain is actually hosted in China but using VPN services to appear located in Hong Kong.

While browsing the site, I encountered pop-up advertisements for prostitution services and the sale of rape drugs and hidden cameras. These links prompted app downloads for further access. I also noticed a banner advertising prostitution services. Following this link revealed a similar structure - a menu page leading to two domains. All prostitution services advertised appear to be based in China, where both prostitution and pornography are illegal. The domains for these services (<https://anger.mdknqszb.cc/> and <https://appear.mehteuwx.cc/>) showed a risk score of 81, the same registrar as previous domains ([abuse@godaddy.com](mailto:abuse@godaddy.com)), suspiciously recent creation (only 5 days old), and an IP address located in Hong Kong.

Further research revealed that [abuse@godaddy.com](mailto:abuse@godaddy.com) is associated with GoDaddy’s account management page, which includes a mechanism for reporting illegal domains. Given the nature of the content and services being hosted, reporting these domains to GoDaddy would be appropriate. So should I fill a report?