Too big to care? - Our disappointment with Cloudflare's anti-abuse posture

spamhaus.org/resource-hub/service-providers/too-big-to-care-our-disappointment-with-cloudflares-anti-abuse-posture/

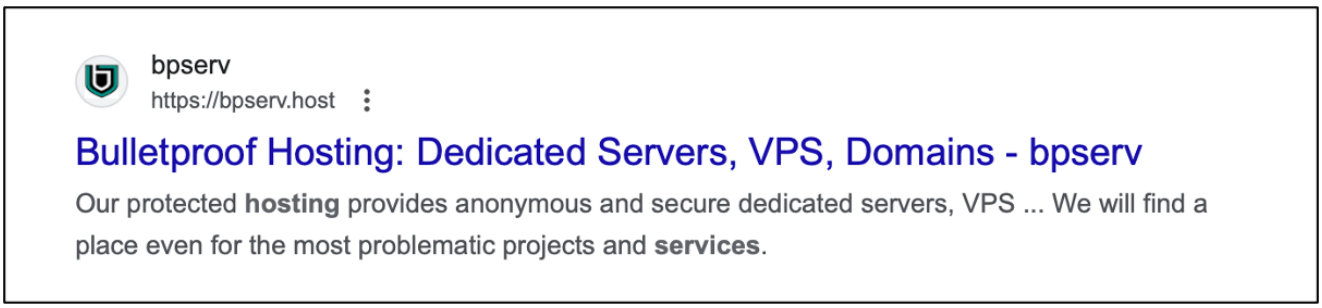
What Spamhaus is seeing

For years, Spamhaus has observed abusive activity facilitated by Cloudflare's various services. Cybercriminals have been exploiting these legitimate services to mask activities and enhance their malicious operations, a tactic referred to as living off trusted services (LOTS) [2].

With 1201 unresolved Spamhaus Blocklist (SBL) listings [3], it is clear that the state of affairs at Cloudflare's Connectivity Cloud looks less than optimal from an abuse-handling perspective. 10.05% of all domains listed on Spamhaus's Domain Blocklist (DBL), which indicates signs of spam or malicious activity, are on Cloudflare nameservers [3]. Spamhaus routinely observes miscreants moving their domains, which are already listed in the DBL, to Cloudflare to disguise the backend of their operation, be it spamvertized domains, phishing, or worse.

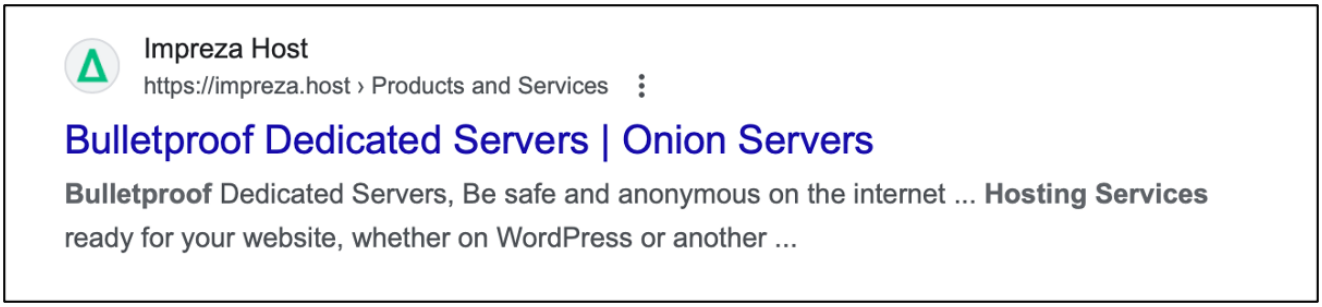
Further investigations

Research into websites that are openly advertising services to a cybercriminal audience, such as bulletproof hosting, reveals that many of these domains are supported by Cloudflare's services. As an example, task your trusted search engine with searching for bulletproof hosting [4], and you will find that many of the domains returned are, in fact, hosted on Cloudflare's nameservers:



bpserv.host. 3598 IN NS lloyd.ns.cloudflare.com

bpserv.host. 3598 IN NS brit.ns.cloudflare.com



impreza.host. 21600 IN NS chan.ns.cloudflare.com

impreza.host. 21600 IN NS lex.ns.cloudflare.com

Repeat this with other cybercriminal offerings of your choice - such as carding forums, DDoS-for-hire services, and worse - and the results will be similar.

For a certain domain registrar, every single domain Spamhaus has observed appearing on Cloudflare's nameservers thus far is associated with phishing—a campaign continuing for months on end.

Cloudflare's anti-abuse conundrum

Cloudflare's approach to abuse is described on a web page, and further explained in this article published in August 2022. The troublesome point of their policy is: "The vast majority of abuse reports that we receive are about websites using our pass-through security, and content distribution network (CDN) services. Cloudflare does not host content through those services, and we cannot remove content from the internet that we do not host. Our abuse reporting system is therefore designed to ensure that your report gets to the parties best positioned to address your complaint: the website operator and the hosting provider for the website on which the content is posted."

From a technical perspective, this approach might seem logical - however, Spamhaus is not asking Cloudflare to remove content from the internet, and other entities with an understanding of the principles of a CDN are unlikely to do so either. Rather, the request is for Cloudflare to stop providing their pass through services to abusive actors.

Unfortunately, from an abuse-handling perspective, their approach is problematic. Cloudflare effectively masks the true location of the backend where services are being hosted, while passing on any complaints about abuse to the abused or abusive services. As a result, notifications to customers may end up going directly to the abuser, who can proceed to ignore them and, at the same time, refine their strategies to avoid further detection.

Alternatively, the notifications may go to an intermediate actor like a hosting provider who, wholly screened from the public eye by the Cloudflare service, needs a solid motivation to terminate a paying customer that is not in the slightest deteriorating their reputation. The

intermediate actor is then likely to ignore the notification or pass it over to the abusing customer and forget about it.

The risk of this policy is that it could be perceived as facilitating a “bulletproof [hosting] service,” where the only visible internet resources associated with the abusers are (i) Cloudflare’s and (ii) unstoppable by policy.

Why does Cloudflare take this approach?

The advantage of this policy is that it makes life easy for Cloudflare, as they do not have to do any deep investigation or analysis of incidents, and notification flow can be largely automated. In this way, the cost of dealing with abuse is very low, benefiting the bottom line. Unfortunately, the effects of such an approach are felt negatively by the rest of the internet.

How Cloudflare can resolve this issue

After receiving evidence of abuse, we’d recommend Cloudflare suspend services to the abusers: namely, the authoritative DNS service to their domain(s), the reverse proxy services, and the CDN services. By doing this, contents would remain in the same place where they were before (unknown to everyone except Cloudflare), but would no longer be accessible through the Cloudflare network.

A more detailed explanation of how ISPs can battle fraudulent sign-ups can be found here in a blog post published by Spamhaus in 2012.

A call for change

Being recognized as a leader in today’s Content Delivery Network (CDN) market, Cloudflare has the tools and resources to provide robust services to legitimate customers, while keeping all the cybercriminals off its premises.

Compared to small ISPs, they do not face constraints that make having a decent abuse desk prohibitively costly. The vast majority of abusive activity can be prevented upfront – in many cases, even without any human interaction. In light of this discrepancy, Cloudflare’s and similar companies’ current anti-abuse posture is weakening trust and safety.

Spamhaus has always stressed that abuse does not “just happen” – it is enabled.

So, please, Cloudflare, and all those who run services from which miscreants “live off,” improve your abuse prevention and abuse handling – swiftly and significantly. We’re here to work together to strengthen trust and safety for the internet, and welcome working with all organizations in that endeavour.

[1] Spamhaus uses the services of Cloudflare. In fact Cloudflare helped Spamhaus during one of the worst DDoS attacks in the history of the internet, back in 2013. We were, and continue to be grateful, for the services Cloudflare provides us. Our concern is with how Cloudflare handles and prevents abuse. From a short-term business operating perspective, declining to tackle abuse makes financial sense. However, from a longer term brand and business continuity perspective, it presents significant challenges.

[2] Known more properly as, “living off trusted sites” - see our blog post.

[3] At the time of publishing.

[4] Spamhaus defines bulletproof hosting – a SBL listing criteria – as “DNS, web, mail or other services provided with either explicit or tacit actions not to disconnect customers who spam or engage in cybercrime.”