Website IP privacy for free, this may help mitigate some web attacks

A quick presentation by Austin Bollinger

Cloudflare

An affordable plan for individuals and small business is free. The FBI uses Cloudflare to enhance their web delivery and security. If you want more advanced security features like a WAF (web application firewall), that is an upgrade charge or you could roll your own open source with time configuring e.g. ModSecurity, IronBee, NAXSI, WebKnight, Shadow Daemon.

Stop HTTPS leaking your domain's IP

Therefore, you get setup behind Cloudflare and route all traffic through Cloudflare's proxies to hide your IP. Not so fast, using free tools like Censys and Shodan someone can easily pull your IP from a quick HTTPS grab if you have configured a website with default configurations. Two solutions: vhost properly and restrict all traffic to the server's web ports except via Cloudflare's IP addresses.

Now our IP is tucked away safely or no

Inbound, everything is locked down in terms of IP privacy. Common mistakes are setting up subdomains without usage of the Cloudflare proxy thus leaking the web server IP anyway and outbound IP sending. Let us say for example you have a newsletter being sent out from your website example.com and you decided to use Sendmail or Postfix locally or even remotely. We want IP privacy, right? Ouch! Email headers just dropped your web server IP to a potential attacker's email.

Like all tech security 'stuff', CHECK YOUR **INPUT/OUTPUT**! Then again including your bounds.

Like above mentioned, inputs are on lock aside from anything cached. Although typically unnecessary, one may also change their IP addresses on affected systems. To protect your web server IP, we need email to not hand out our web server IP. Gmail is going to have an origin IP, default configured remote Postfix relay is going to have your web server IP, and many SMTP providers will have origin IP addresses. Business solutions exist at a price; I understand the need for affordable small business options. I am happy to share that a Postfix remote relay can effectively filter IP using smtp_header_checks, for example in your main configuration add

```
smtp_header_checks = regexp:/etc/postfix/header_checks
```

Then you can set IGNORE to "Received", "X_PHP-Originating-Script", "Message-Id" and so on. **Time up**!

DISCLAIMER: The information contained in this document is not legal advice and is for informational and/or educational purposes only.