HOME CYBER DEFENSE
ARE YOU SAFE FROM CYBER CRIME?
ALERT

Issued 2/27/17

What You Need Know About the Cloudflare Data Leak

Cloudflare revealed a bug in its code caused sensitive data to leak from major websites that use its services, including big names such as Uber, Fitbit, 1Password, and OkCupid. There are an estimated 4.2 million domains using Cloudflare, which may have leaked data, including crypto keys, passwords, user sensitive information, and so on. The list is long and includes many big name services, as well as torrents, bitcoin sites, and so on.

The bottom line is that no one really knows at this point exactly how many sites were affected by the data leak, especially since the information bled out over the course of five months before being discovered by Google's Tavis Ormandy. Google, Yahoo, Bing and other search engines have worked on scrubbing the data before Cloudflare went public with the bug in order to protect people from hackers taking advantage. Researchers are still finding samples of leaked data in search engine caches, however, so it's clear the problem is not completely solved. Security researcher Hector Martin tweeted that you can still find random authentication cookies for sites affected by Cloudbleed with a simple Google search, and the worst part is that they work.

The name Cloudbleed is, of course, the name given to the incident inspired by the HeartBleed OpenSSL security issue from a few years back.

Cloudflare says that no one before Tavis Ormandy discovered the bug before so there might be some hope that eventually all data will be scraped.

The company claims that the leak was at its worst for less than a week when 1 in 3.3 million Cloudflare requests might have caused leakage, which is 0.00003% of requests. As of right now, however, it's best that you take steps to protect yourself. First off, you would be better off checking whether the sites you use most are on the list of services potentially affected by CloudBleed.

There's a list put together by a GitHub user Pirate of all sites that use Cloudflare's services. Patreon, 4chan, Medium, Bitpay, News.ycombinator.com, uber.com, Yelp.com, uber.com are just some of the many sites on the list. There's also a tool available online called DoesItUseCloudflare to check on specific sites. You can go and see if the one site you're worried about is affected. If it is, you'll get a message in a red box telling you that the site was subject to CloudBleed, if not, the message comes in a green box.