Cloudflare introduces tools to detect new HTTPS blocking

Cloudfare has recently released 2 new tools designed to simplify the process of checking whether TLS connections to the website are blocked.

Cloudfare has recently released 2 new tools designed to simplify the process of checking whether the TLS connections to the website are blocked and at the same time detecting vulnerable and available clients. the ability to send notifications to clients when their security systems are compromised, or are obsolete, degraded.

The reason behind blocking HTTPS can also be harmless or malicious, and it often happens when Internet connections go through proxy or middlebox instead of connecting the client directly to the server, leading to a situation. Cloudfare called "monster-in-the-middle".

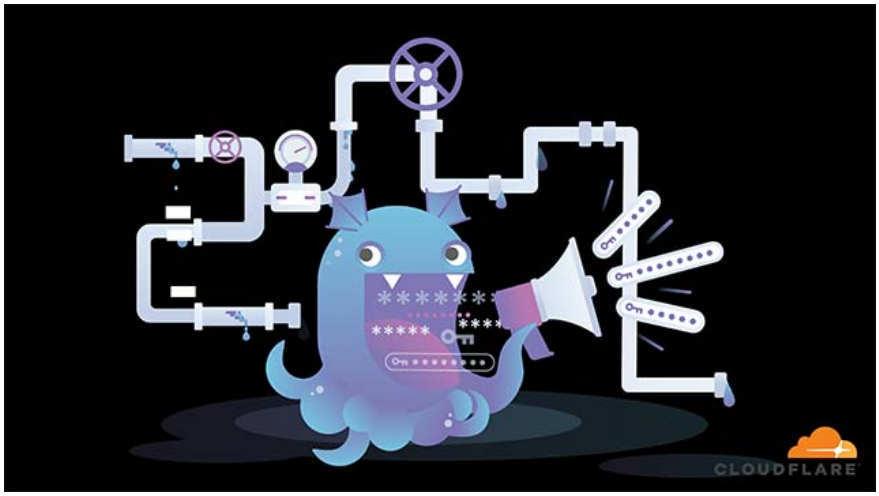
1. Google Chrome on Android has just been updated, doubling the page loading speed, saving up to 90% data usage

An article investigating the security impact of HTTPS blocking since 2017 shows that the blocking behavior of HTTPS connections is spreading dramatically, with "62% of traffic through the middlebox being lost. security features and 58% connect the middlebox containing serious vulnerabilities ".

New tools to detect and analyze blocked TLS connections

In addition, after considering the behavior and behavior of antivirus programs and many companies operating in the field, the researchers found that "nearly all have self-degradation in the connection secret and contains a lot of vulnerabilities (eg Certificate authentication failed) ".

Cloudfare has announced 2 new tools. An open source library for detecting HTTPS blocking behaviors called MITMEngine and a digital interface table showing statistics about blocked TLS connections according to Cloudflare's observation on the service provider's network This case, called MALCOLM.



1. Websites that use HTTP protocol will have to switch to HTTPS if they do not want to "leak" and "blacklist" Google

According to Cloudflare experts, HTTPS blocking can occur when devices that come with the original certificate are installed to allow third parties to decrypt and check Internet traffic, or when The root providing its own TLS private key to a third party (such as a reverse proxy) is responsible for blocking TLS connections.

In general, HTTPS blocking may occur because:

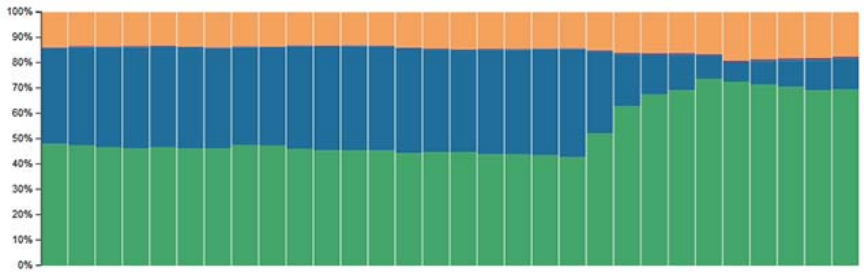
1. Antivirus and proxy tools are designed to detect inappropriate content, malware and data breaches.
2. Proxy software can steal sensitive information while injecting content into web traffic at the same time.
3. The reverse proxy is used by the root server to improve the security of HTTPS connections on the client.

Golang - Cloudfare's HTTPS MITMEngine blocking behavior detection library - designed specifically to help determine the cause and ability of HTTPS connectivity is blocked on an Internet connection using User Agent and authenticating fingerprints TLS Client Hello.

By looking for differences on all the collected information, MITMEngine can provide "the most accurate detection of blocking HTTPS and getting fingerprints TLS", knowing when HTTPS connections are blocked, Which software the attacker may have used.

1. Enhance the effectiveness and security of Website with CloudFlare

Besides, Cloudfare also introduced the MALCOLM interface panel, a publicly accessible tool designed to display "HTTPS blocking statistics collected by MITMengine (Monster-In-The-Middle tool). - 'detector' of HTTPS blocking behavior of Cloudflare. "



HTTPS interception detected (Orange:Yes, Green: No, Blue: Unknown)

In the chart above, it can be seen that Cloudfare has tracked the percentage of HTTPS connections blocked on its network for the last 30 days. In it, orange is blocked, blue is unbounded and green is undefined. As detailed in the blog post, Cloudfare explains that an unknown state is created when there is no "fingerprint referring to a specific browser or bot; therefore, we cannot evaluate whether there is whether HTTPS blocking behavior occurs ".

You can read more about these two tools at: blog.cloudflare.com/monsters-in-the-middleboxes

You finished reading the article "**Cloudflare introduces tools to detect new HTTPS blocking**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.