Blocked Site Alerts for TLS

Ted Lemon <ted.lemon@nominum.com>

draft-lemon-tls-blocking-alert-00

Problem statement

Not all connections are safe for the end user

There is a perceived need to provide blocking services, which prevent end users from connecting to malicious sites online

Other factors can motivate blocking access to the network--e.g. Failure to pay

UX for these blocks is poor: the user has no idea why the site isn’t working, or gets an “invalid cert” warning they have to click through to gain access.

What people are doing

Just block TLS connection and send a access denied

Instruct the end-user to install a cert that enables MiTM-ing connections

Instruct the end-user to click through certificate warnings (or, status quo, this just happens because of the way the protocols operate)

This is bad

Bad UX leads to costly support calls, which motivates more drastic solutions

MiTM-based solutions put end-users at risk

Training users to click through cert warnings is worse

What can we do?

Nothing

Provide better UX

Nothing

This will almost certainly result in site blocking systems doing things that compromise user security. We can wash our hands of it, but if we do, we are ignoring a real threat to user security. There isn't someone else who can address this problem.

Provide better UX

Any message from a device in the middle is by definition an attack

Therefore, allowing the “attacker” to choose a payload that is shown to the user presents an attack surface--some users can be talked into making serious mistakes.

Alert codes offer a compromise: “attacker” can choose a result code, but the result code contains no data the user will see other than a standard set of result codes for which we have done some threat analysis.

Proposal

Draft-lemon-tls-blocking-alert-00

This document adds a number of result codes to indicate common reasons why a TLS connection might be blocked.

Response on mailing list: we shouldn’t cooperate with this

If not, aren’t we cooperating with something worse?

Is there some other concrete solution to this problem that I am missing?