Browser Pivoting

Archived: 2026-04-05 21:18:55 UTC

Malware like Zeus and its variants inject themselves into a user's browser to steal banking information. This is a man-in-the-browser attack. So-called, because the attacker is injecting malware into the target's browser.

Overview

Man-in-the-browser malware uses two approaches to steal banking information. They either capture form data as it's sent to a server. For example, malware might hook PR_Write in Firefox to intercept HTTP POST data sent by Firefox. Or, they inject JavaScript onto certain webpages to make the user think the site is requesting information that the attacker needs.

Cobalt Strike offers a third approach for man-in-the-browser attacks. It lets the attacker hijack authenticated web sessions—all of them. Once a user logs onto a site, an attacker may ask the user's browser to make requests on their behalf. Since the user's browser is making the request, it will automatically re-authenticate to any site the user is already logged onto. I call this a browser pivot—because the attacker is pivoting their browser through the compromised user's browser.

figure 63 - Browser Pivoting in Action

Cobalt Strike's implementation of browser pivoting for Internet Explorer injects an HTTP proxy server into the compromised user's browser. Do not confuse this with changing the user's proxy settings. This proxy server does not affect how the user gets to a site. Rather, this proxy server is available to the attacker. All requests that come through it are fulfilled by the user's browser.

Source: https://www.cobaltstrike.com/help-browser-pivoting