

Original URL: http://www.theregister.co.uk/2008/09/11/cookiemonster_rampage/

CookieMonster nabs user creds from secure sites

By [Dan Goodin in San Francisco](#)

Published Thursday 11th September 2008 02:41 GMT

Websites used for email, banking, e-commerce and other sensitive applications just got even less secure with the release of a new tool that siphons users' authentication credentials - even when they're sent through supposedly secure channels.

Dubbed CookieMonster, the toolkit is used in a variety of man-in-the-middle scenarios to trick a victim's browser into turning over the authentication cookies used to gain access to user account sections of a website. Unlike an attack method known as [sidejacking](#) (http://www.theregister.co.uk/2008/02/01/google_ssl_sidejacking/), it works with vulnerable websites even when a user's browsing session is encrypted from start to finish using the secure sockets layer (SSL) protocol.

According to Mike Perry, the creator of CookieMonster, websites that appear to be vulnerable to the attack include united.com, bankofamerica.com, register.com, netflix.com, and a host of other big-name online destinations. Errata Security's Rob Graham, who introduced Sidejacking tools a little more than a year ago, says Gmail is not vulnerable as long as a recently implemented [https-only option](#) (http://www.theregister.co.uk/2008/07/25/gmail_adds_https_only/) is turned on. However, Google Docs, Google's Blogger.com and Google Finance remain wide open.

The vulnerability stems from website developers' failure to designate authentication cookies as secure. That means web browsers are free to send them over the insecure http channel, and that is exactly what CookieMonster causes them to do. It does this by caching all DNS responses and then monitoring hostnames that use port 443 to connect to one of the domain names stored there. CookieMonster then injects images from insecure (non-https) portions of the protected website, and - voila! - The browser sends the authentication cookie. (For a more detailed explanation of how it works, see [this link](#) (<http://fscked.org/blog/3>).

For now, CookieMonster is in the hands of only about 225 security professionals. In the next couple of weeks, he plans to make it generally available. Perry says he hopes the limited release will help spread the word that this vulnerability needs to be fixed sooner rather than later.

While Perry has listed some two-dozen sites that are vulnerable, we are betting the list is much, much bigger. To find out if your bank is susceptible, clear all cookies and then log in to the site. Next, clear all cookies marked as "SECURE" (in Firefox, go to preferences > privacy > show cookies. Delete only the cookies marked as "Encrypted connections only"). Then visit the site again. If you are logged in, there is a strong chance the site is wide open.

If you find any, feel free to report it as a comment. ®