Drive-By Pharming is a hacker attack aimed at the home market and could steal your banking details….

So get your wireless router properly secured now!

Pharming is a malicious hacking technique where an attacker redirects a user from a legitimate Web site to a bogus Web site that contains malicious code. In this new drive-by pharming attack, aimed at home web users, the malicious hacker steals banking passwords and login details, which were destined for legitimate sites.

In this variation on other drive-by hack techniques, attackers use a malicious web site to remotely reconfigure home broadband routers. The attack can only work when a broadband router is not password-protected, or an attacker is able to guess the password. But because most routers come with well-known default passwords, that users don't bother to change, the potential number of victims who might fall prey to drive-by pharming is vast; some estimates say up to 50% of home web users may be at risk.

With traditional pharming, an attacker redirects a user from a legitimate web site to a bogus web site that contains malicious code. Pharming attacks can be executed by either changing the host file on a victim's PC or manipulating a domain name system (DNS) server.

In the new scheme, when a user visits a malicious Web site, an attacker is able to remotely change the (DNS) settings on the broadband router or wireless access point, and re-route requests for legitimate sites, like online banking or financial institutions, to bogus sites designed to steal login information.

This new attack exposes a problem affecting millions of broadband users worldwide, because of the ease with which drive-by pharming attacks can be launched, it is vital that consumers adequately protect their broadband routers and wireless access points straight away.

Router Control

If an attacker can trick you into visiting his page, he can probe your machine.

Here's how the drive-by pharming attack works: Once the user clicks on a malicious link, JavaScript code is used to change the (DNS) settings on the user's router. From that point on, every time the user browses to a web site, the request will be satisfied by the attacker's server.

This gives the attacker complete discretion over which web sites the victim visits on the Internet. For example, the users might think they are visiting their online banking web site but in reality they have been redirected to the attacker's site. These fraudulent sites are almost exact replicas of the actual site, so the user will be unlikely to recognise the difference.

Once the user is directed to the pharmer's "bank" site, and enters a username and password, the attacker can steal this information. The attacker will then be able to access the victim's account on the real bank site and transfer funds, create new accounts, write cheques, and so forth.

Hitting the Brakes

What's important to remember is that this drive-by pharming scheme is an attack, not a vulnerability. It relies on social engineering and lack of proper security controls, but does not take advantage of a security flaw.

Because the issue is not vulnerability, existing security solutions on the market cannot protect against it. Drive-by pharming targets the user's router directly, and the existing solutions only protect the user's computer system.

Computer users should make sure their routers have unique passwords.