



ABA News to Use

Keeping banking's frontline personnel informed

Drive-by Pharming Poses Security Threat to Home PC Networks

Symantec Corp., which produces PC security software tools, and Indiana University's School of Informatics recently announced a significant new computer security threat called drive-by pharming.

Under this scam, consumers may fall victim to pharming -- online thieves harvesting computer users' personal information and passwords -- by having their home broadband routers reconfigured by a malicious Web site. According to a separate informal study conducted by Indiana University, up to 50 percent of home broadband users are susceptible to this attack.

With traditional pharming, an attacker aims to redirect a user attempting to visit one Web site to another, bogus, Web site. Pharming can be conducted either by changing the host file on a victim's computer or through the manipulation of the Domain Name System, or DNS. In drive-by pharming, a user visits a malicious Web site and an attacker is then able to change the DNS settings on the user's broadband router or wireless access point.

Drive-by pharming is made possible when a broadband router is not password protected or an attacker is able to guess the password -- for example, most routers come with a well-known default password that a user never changes.

"This new research exposes a problem affecting millions of broadband users worldwide," said Oliver Friedrichs, director of Symantec Security Response. "Because of the ease by which drive-by pharming attacks can be launched, it is vital that consumers adequately protect their broadband routers and wireless access points today,"

Drive-by pharming involves the use of JavaScript to change the settings of a user's home broadband router. Once the user clicks on a malicious link, malicious JavaScript code is used to change the DNS settings on the user's router. From this point on, every time the user browses to a Web site, DNS resolution will be performed by the attacker.

DNS resolution is the process by which one determines the Internet address corresponding to a Web site's common name. This gives the attacker complete discretion over which Web sites the victim visits on the Internet.

The fraudulent sites are an almost exact replica of the actual site so the user will likely not recognize the difference. Once the user is directed to the pharmer's fraudulent site and enters a user name and password, the attacker can steal this information. The attacker will then be able to access the victim's legitimate commonly visited Web sites.

To protect themselves, computer users should:

-- Make sure their routers are uniquely password protected. Most routers come with a default administrator password, which is easy for pharmerms to guess.

--Use an Internet security solution that combines antivirus, firewall, intrusion detection and vulnerability protection

-- Avoid clicking on links that seem suspicious -- for example, those sent to you in an email from someone you don't recognize.

The technical details of the attack are described here:

http://www.symantec.com/avcenter/reference/Driveby_Pharming.pdf.

The Symantec Security Response Blog also features a more detailed and technical summary of this attack and how to protect against it, along with a flash animation

describing the attack step-by-step at http://www.symantec.com/enterprise/security_response/weblog/2007/02/driveby_pharming_how_clicking_1.html.

For information about ABA News to Use, or to suggest subjects for future articles, please contact ABA's [Brian Nixon](#).