MIT Technology Review

Rerouting the Router

Researchers have found a new way for attackers to change critical settings on home routers.

February 26, 2007

Security experts have discovered a new kind of computer attack that could affect millions around the world. A simple website can be made to manipulate household routers–used to connect multiple home computers to the Internet–so that scammers can gather personal information and passwords.

Rogue code: Security researchers have proved that a new kind of computer attack is possible. Code hidden in a Web page can be used to infiltrate home routers and change the domain-name settings.

According to researchers from Indiana University and the antivirus software company Symantec, anyone with a little skill can search for vulnerable home routers and change critical settings so that real websites are secretly replaced with bogus pages asking for log-in information.

"The big problem is that you can't immediately see that there is a problem," says Sid Stamm, a Ph.D. candidate at Indiana University's School of Informatics and one of the researchers on the project.

For example, an unknowing victim who types in the domain name of his or her bank might be greeted by a page that looks legitimate. But any log-in and password information that is entered on that page would go straight to the scammer.

At its core, the attack is an old ploy called pharming. But Stamm and his colleagues found a new twist: a Web page, they say, can be used to launch an attack against home routers and manipulate domain-name server settings. (There has been previous speculation that this kind of attack might be possible, but the researchers say they are the first to prove that a Web page can be used to reconfigure these particular settings on the router.) All the attacker needs is the user's internal Internet Protocol (IP) address and the password for the configuration settings on the router. Both, Stamm says, can often be easily acquired in a remote, automated attack.

First, the attacker sets up a Web page to lure victims with popular content, such as celebrity photos, says Zulfikar Ramzan, a senior principal researcher at Symantec who also worked on the router project. While the victim views the pictures, unseen code nabs the user's IP address and probes the router, looking for clues that might reveal its brand. A picture of the company's logo, for example, is usually saved on the router. All this poking around doesn't raise any red flags because the router thinks it's all just legitimate requests for information from the victim's home computer.

Once the attacker determines the router's brand, he or she can often guess the configuration password because many people use the manufacturer's default, Stamm says. While it's not known exactly how many routers lack adequate configuration passwords, an informal study published last year in the *Journal of Digital Forensic Practice* found that 50 percent of home users with a broadband Internet router either opted for the default or didn't have a password at all. (Routers have another optional password to stop outsiders from using a wireless network, and people frequently don't employ that password system either. But it is the configuration password specifically that is used in this attack.)

With the configuration password and IP address, the attacker can easily change which domain-name server the victim uses as an Internet directory. "It's like the attacker has replaced your phone book with a new one," Ramzan says. "So now you're getting addresses from the attacker's phone book."

The next time the victim goes to his or her bank's website, for example, the Web browser might be redirected to an imitation site. This fake site, run by the attacker, is used to capture the victim's log-in and password information.

Ramzan insists that this wouldn't take a lot of skill. "This particular attack is very powerful in that regard. The attacker doesn't have to be that technically sophisticated to mount it."

Fortunately, fixing the problem is also simple. "The easiest way to defend against this kind of attack is to change your [router's configuration] password," says Ramzan. Unfortunately, router manufacturers don't require users to establish new passwords because they want their software to be easy to use.

"They wanted to simplify the process, so they made it so that people weren't really prompted or encouraged to change the password," Ramzan says. "My feeling is that it's a pretty easy change [for the router companies] to make."

Another easy fix: make the default password unique. The password could, for example, be set initially to the product's serial number. While the attacker could still attempt to guess at the serial number, each failed log-in attempt would alert the user with an error message.

But Ramzan says the root of the problem isn't the configuration password. The real issue is that a Web page can be used to reconfigure a router's settings at all. That, he says, is what security experts will need to address going forward.

The router researchers say that they haven't yet seen anyone actually launch such an attack, and they hope their work will raise awareness so that people change their passwords before it becomes a real issue.

"It's an interesting discovery," says Jeff Gennari, an Internet security analyst with CERT, a computer-security coordination center established by various U.S. federal agencies, including the U.S. Department of Defense, and run by Carnegie Mellon University's Software Engineering Institute. "Uncovering these types of configuration problems brings to light how complicated security can be."