Hacker pierces hardware firewalls with web page

Dan Goodin in San Francisco

6th January 2010

On Tuesday, hacker Samy Kamkar demonstrated a way to identify a browser's geographical location by exploiting weaknesses in many WiFi routers. Now, he's back with a simple method to penetrate hardware firewalls using little more than some javascript embedded in a webpage.

By luring victims to a malicious link, the attacker can access virtually any service on their machine, even when it's behind certain routers that automatically block it to the outside world. The method has been tested on a Belkin N1 Vision Wireless router, and Kamkar says he suspects other devices are also vulnerable.

"What this means is I can penetrate their firewall/router and connect to the port that I specified, even though the firewall should never forward that port," Kamkar told *El Reg*. "This defeats that security by visiting a simple web page. No authentication, XSS, user input, etc. is required."

Kamkar's proof-of-concept page forces the visitor to submit a hidden form on port 6667, the standard port for internet relay chat. Using a hidden value, the form surreptitiously coerces the victim to establish a DCC, or direct client-to-client, connection. Vulnerable routers will then automatically forward DCC traffic to the victim's internal system, and using what's known as NAT traversal an attacker can access any port that's open on the local system.

For the hack to work, the visitor must have an application such as file transfer protocol or session initiation protocol running on his machine. The hack doesn't guarantee an attacker will be able to compromise that service, but it does give the attacker the ability to probe it in the hope of finding a weak password or a vulnerability that will expose data or system resources.

"Most people have this false sense of security that 'well, I'm behind my router, nobody can

connect to my ports,'" said Kamkar, the hacker behind the notorious Samy Worm that in 2005 took MySpace out of commission by adding more than 1 million friends to the author's account. "If you're going to keep a service open to the world, you'll probably have more upkeep" to make sure it's secure.

Reg readers about what other routers are vulnerable. To test whether the attack can pierce your firewall, visit this page and specify the port of a service that's already running on your system.