Email Injection Bot Attacks and SPF Records

Posted At : November 5, 2005 11:44 AM | Posted By : Mark Kruger
Related Categories: Coldfusion Security, Hosting and Networking

I got an email from someone on my blog about implementing SPF that said it should cut down on email injection attacks. The reasoning was that the email injection attack typically sends "from" the domain of the web site. Since SPF dictates the servers or domains mail can come "from" then mail from the web server would be rejected. Stopping Email Injection Bots would be a nice side effect of SPF, but it is unlikely. This reasoning does not take into account 2 important details.

1. SPF must be implemented on the mail server

It's not enough to just add SPF records to your DNS server, you must configure your mail server to honor them. That's the rub. SPF is a great idea that can help tremendously, but it must gather enough steam to be implemented throughout the net. It has to have some *critical mass* to be truly effective.

2. Web Servers Typically Send Mail Through an SPF Authorized Server

Your web server is probably already configured to send email from your domain through a web server specified in your SPF record. That means, from an SPF perspective, the mail sent (FROM some user in your domain TO some user in your domain and BCC some other user) is actually legitimate.

Always keep in mind that at this point email injection bots don't affect Coldfusion servers - at least not in respect to be able to send out arbitrary email to hidden email addresses (that's the goal of an injection bot). At most they are an annoyance that cause junk messages to appear in the inbox of whoever your form targets for email. Email Injection is really only effective against a PHP server with a weak email script - at least, that seems to be the most likely scenario.

For more information on Email Injection Attacks and cold Fusion see

Contact Us Form - Email Injection Attack
Email Injection Attack Part II