

22 July 2008

By: George Craciun, Security News Editor

## [Sabre Security CEO Figures Out DNS Vulnerability](#)

*Matasano Security acknowledges, then takes it all back*



Halvar Flake may have discovered how the DNS flaw works  
Agder University College

Recently, the [DNS flaw discovered](#) by Dan Kaminsky made all the headlines, first of all because of its gravity, and secondly because the Director of Penetration Testing for IOActive [would not release](#) specific, technical details about the flaw. Kaminsky stated on numerous occasions that he would disclose all the information on the 6th of August, at the BlackHat Security Conference in Las Vegas. But it seems that Thomas Dullien, CEO and head of research with Sabre Security has figured it all out, even though he admits he is not an expert in DNS. This is the message posted on the Matasano Security blog in regard to Dullien's discovery: "The cat is out of the bag. Yes, Halvar Flake figured out the flaw Dan Kaminsky will announce at Black Hat". Halvar Flake is the hacker alias used by Thomas Dullien. It must be noted that the blog post presented above was posted for about five minutes and then it was taken down. Thomas Ptacek from Matasano Security has posted another statement on the site, saying that they "dropped the ball" and it was all a regrettable error. "Earlier today, a security researcher posted their hypothesis regarding Dan Kaminsky's DNS finding. Shortly afterwards, when the story began getting traction, a post appeared on our blog about that hypothesis. It was posted in error. We regret that it ran. We removed it from the blog as soon as we saw it. Unfortunately, it takes only seconds for Internet publications to spread," says Ptacek. According to Halvar Flake, there is no good reason behind Kaminsky's request not to publicly speculate on the DNS vulnerability. He agrees that Kaminsky did the right thing by not disclosing the vulnerability and getting the industry heavyweights to come up with a fix, but by not speculating you are not buying the user any time. "In a strange way, if nobody speculates publicly, we are pulling wool over the eyes of the general public, and ourselves," says [Halvar Flake](#). Dan Kaminsky did not confirm or deny the fact that Halvar Flake had indeed discovered the DNS vulnerability that he came upon earlier this year, and he is urging all users to update, if they haven't done so already. On the 24th Kaminsky will do a webcast for BlackHat, but he says this opportunity will not be used to disclose details on the DNS vulnerability. All those interested in the issue will have to wait until the 6th of August.