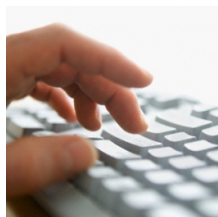


16 October 2007

By: Marius Oiaga, Technology News Editor



## **Don't Trust DNS Servers, Not Even from Windows Vista**

*Or from Mac OS X or Linux, for that matter*

Microsoft's latest operating system Windows Vista was advertised as an epitome of security among Windows platforms. But as the security mitigations and boundaries set up in Vista, or in any other operating system for that matter, including Mac OS X and Linux, become increasingly bulletproof, attackers will turn to secondary avenues of attacks. And in this context, DNS servers can serve as vectors of attack, because the way an URL is sent to the domain name system (DNS) server, which returns the actual address. In this context, a compromised DNS server can easily transform users into victims. "The majority of networks are configured with dynamic host configuration protocol (DHCP). DHCP is a protocol that allows computers to broadcast a generic "configure me" message to the local network. Any server on the network can respond to the message, telling the computer which DNS server to use (among other things). This problem is two-fold: first, there is no guarantee that the response is coming from the expected server. And second, even if it comes from the proper server, what guarantee does the user have that the DNS server provided is actually valid and secure?" asked [Ron Bowes](#), Symantec Security Response Researcher. A hijacked DNS server will present users only with fake websites. From search engines to email services, to online stores and banks. In such a scenario the user can be easily redirected to malicious websites hosting malformed files, malware and exploits, email accounts, passwords as well as credit card information can easily be stolen. "The good news is that sites with SSL certificates will give a warning if the connection is redirected. That is, sites with a "https://" prefix. This means that, if you try visiting your bank site while using a malicious DNS server, your browser will inform you that there's a potential attack taking place. However, most users wouldn't know what this message means or why it's important. The bottom line is that implicit trust in DNS servers is dangerous, because your DNS server, like any other computer, can potentially act maliciously," Bowes added.