

22 July 2006

By: Marius Oiaga, Technology News Editor



Malicious Trojan Disguised as Google Toolbar

The malware will eventually turn a compromised machine into a bot zombie

Online Security Company SurfControl based in Scotts Valley, California, has issued a public warning revealing that it has detected a new malicious threat that impersonates a Google product. SurfControl claims to have identified e-mails disguised as being originated by Google that invite the users to follow up a link that would lead to the installation of the latest variant of Google Toolbar. The use of Google's brand in an attack translates into consumer confidence and a human based vulnerability. The link comprised in the e-mail leads to a spoofed Google Toolbar Web site that apparently offers the Mountain Views Company's toolbar. In actuality, the fake page delivers a Backdoor Trojan instead of the Google Toolbar plug-in. The fake Google Toolbar Web was spoofed correct addresses, and SurfControl warned that the hackers made use of Google's redirection service to hide the real addresses. Users downloading the malicious Toolbar will become infected with Backdoor Trojan W32.Ranky.FW. The malware will eventually turn a compromised machine into a bot zombie. SurfControl did not rank the threat with a high level, partly because the attempt is a poor programming compilation and defective in achieving its purpose. The company claims that it has toned its security products in accord with the new threat and that its customers are well protected.