

19 June 2006

By: Marius Oiaga, Technology News Editor

**MailScan**

[Doombot.k Worm Attack via "Abuse" E-mail](#)

It spreads via phishing model attack

MicroWorld Technologies online security company has issued a warning in which announces that a new type of Backdoor Worm named Doombot.k is rapidly spreading via "abuse warnings" e-mails, spoofing domain names of security software companies in order to spread through a phishing method. Once it has compromised a system, the worm stays active in the background due to IRC both capabilities and functions as a Backdoor Server, allowing remote access to the PC and lowering the security level. From there it spreads via mass mailing using the data in the victims computer to send copies of itself as .pif, .scr, .exe, .cmd and .bat attachments to all e-mail addresses in the user's address book. At this level the worm also spoofs the domain name under sender and identifies it with the domain of the harvested email address. Account Alert, Important Notification, Members Support, Notice of account limitation, and Security measures are the subjects displayed by the Doombot.k in order to determine the users to open the compromised files. "This is a fine instance of what we call as the Convergence of Online Crimes," says Govind Rammurthy, CEO, MicroWorld Technologies. "You've got an attack that resembles phishing, which spreads an email worm that eventually creates large botnets, to be used as hotbeds of online crimes. It clearly indicates that in the dark under-belly of Internet, criminals are connecting, grouping and organizing all sorts of malicious activities with clear financial and informational motives."