

Doombot Worm Spreads via Phishing Model Attack

Released by: Manish Katara
Web Site: <http://www.mwti.net>
MicroWorld Security News



Email: manish@mwti.net
Keywords: [antivirus](#), [content security](#), [malware](#), [adware](#)
Update Date: 6/16/2006 4:30:16 PM
Hits: 17

Description:

Security experts at MicroWorld Technologies inform that a Backdoor Worm named 'Doombot.k', is spreading fast via 'abuse warning' emails, spoofing domain names of security software companies and leading business houses. The modus operandi of proliferation is strikingly similar to many phishing attacks in recent times.

Doombot.k comes with IRC bot capabilities and spreads via mass mailing. Once inside the computer, the worm runs in the background, acting as a Backdoor Server that provides access to the victim's PC via IRC channels, for the remote attacker. The smart worm also lowers the security level of the computer, and changes entries in the Windows HOSTS files in order to block websites of AntiVirus companies.

For its spreading routine, the worm steals email IDs from the victim's address book and starts sending itself as .pif, .scr, .exe, .cmd and bat attachments. The most interesting aspect noted here is that it spoofs the domain name of the sender to the same domain of the harvested email address. For example, if the worm steals an email address 'john@xyz.com', it will fake the sender's id as 'abuse@xyz.com', or 'security@xyz.com' and will send it to John's mail address. In the internal email system of enterprises, this can wreck havoc by spreading fast to infect the entire network.

The subject line of the email is picked from a list that includes various titles like-'Account Alert', 'Important Notification', 'Members Support', 'Notice of account limitation', and 'Security measures'.

The body of the message too is chosen from a list of five options. One of them threatens the user that if the user doesn't follow the link and confirm the authenticity of the account, it will be terminated. It directs you to two links, one of which throws up an error page and the other, the Doombot Worm in 'Pif' format.

In the last few months, MicroWorld has detected a large number of Trojans and Worms that can create bots out of user PCs. Botnets are formed by a network of such computers taken over by hackers, to launch, direct and manage fraudulent activities, online crimes and malicious attacks. The security firm that produces the world's most advanced security software solutions, reported a three fold increase in the number of bots across the globe in the year 2005, compared to 2004.

"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."

MicroWorld:
MicroWorld (www.mwti.net) is the developer of the world's first Real-Time Anti-Virus and Content Security software eScan for desktops and servers. Its communication security software, MailScan is the first comprehensive e-mail scanner for your SMTP/POP3 Mail Server. MicroWorld Winsock Layer (MWL) is the revolutionary technology underlying these products, powering them to several certifications and awards by some of the most prestigious testing bodies, notable among them being Virus Bulletin, Checkmark, TUCOWS, Red Hat Ready, and Novell Ready. Combining their powerful scanner with MWL technology, MicroWorld solutions provide a Real-Time Proactive security for your systems. For network security of enterprises, eConceal Firewall is the latest powerful offering from MicroWorld.

To learn more, kindly visit <http://www.mwti.net>

Contact information:
sales@mwti.net