



[Home](#) | [Forums](#) | [Archives](#) | [Search](#) | [Speedtest](#) | [Advertising](#) | [Contact](#) | [About & Link](#) | [RSS](#)

Links

- [Home](#)
- [Have your say](#)
- [Blogs](#)
- [Podcast](#)
- [Downloads](#)

Categories

- [Telecoms](#)
- [Broadband](#)
- [ADSL](#)
- [3G & Cellular](#)
- [MyWireless](#)
- [iBurst](#)
- [Gaming](#)
- [Hardware & Software](#)
- [International Business & General](#)

News Partners

[Home](#) ▸ [3G & Cellular](#)

HETZNER
Trusted in Hosting

DEDICATED SERVER SPECIAL

- R1 195 per month (entry level)
- 5GB monthly traffic
- 9c per additional MB
- Month-to-month contracts

Free setup
save
R2 850

Doombot worm spreads via phishing model attack

By ICTWorld, 20 June 2006



MicroWorld Technologies says that a backdoor worm named 'Doombot.k', is spreading fast via 'abuse-warning' e-mails, spoofing domain names of security software companies and 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 Web sites of ant-virus companies.

For its spreading routine, the worm steals e-mail 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 e-mail address.

For example, if the worm steals an e-mail address 'john@xyz.com', it will fake the

Related Articles

- [HSDPA now in 50 countries](#) 06/20/06
- [Nokia, Siemens merge to close gap on Ericsson](#) 06/20/06
- [Upgrade for ECape cell coverage](#) 06/20/06
- [Nokia, Siemens merge to close gap on Ericsson](#) 06/19/06
- [Nokia launches new 3G phones](#) 06/19/06
- [Nokia to demonstrate 3.6 Mbps HSDPA](#) 06/19/06
- [MTN aims to become broadband leader](#) 06/19/06
- [Virgin Mobile prepares for SA debut](#) 06/15/06
- [Divvying up the digits](#) 06/15/06
- [Phase in new cell phone saw, urges chamber](#) 06/15/06

Sponsor

[Financial Mail](#)

[Business Day](#)

[Business Report](#)

[MoneyWeb](#)

[ICT World](#)

[Finweek/Fin24](#)

Sponsor

sender's ID as 'abuse@xyz.com', or 'security@xyz.com' and will send it to John's mail address. In the internal e-mail system of enterprises, this can wreak havoc by spreading fast to infect the entire network.

The subject line of the e-mail 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 does not follow the link and confirm the authenticity of the account, it will be terminated. It directs users to two links, one of which throws up an error page and the other, the Doombot Worm in 'Pif' format.

© 2006 MyADSL, All Rights Reserved.



Platinum
ADSL
for sheer
internet pleasure
DataPro
INTERNET SOLUTIONS FOR THE REAL WORLD
click here

News Discussions

Advertisement