

# IT Backbones™

## Security News



Give your mouse a heart!

search 

The IT Shield - Dedicated To IT Security Issues, Featuring News, Press Releases, IT Directory & Links

- [Home](#)
- [About](#)
- [Contact](#)
- [Submit PR](#)
- [Search News](#)
- [What We Can Offer You](#)
- [IT Events](#)
- [Time & Money](#)

## Worm Spreads In China Via New Vulnerability In Windows

Published 18th August 2006

It's become real. The much feared mass-level attack of the Backdoor-Worm Win32.IRCBot.st is underway in China, affecting thousands using Shanghai Telecom's broadband services since its outbreak on Tuesday evening, inform Security Experts at MicroWorld Technologies.

Known as 'Worm.Mocbot' or 'Devil Wave' in Chinese media, this worm is a variant of 'IRCBot.st' that exploits vulnerability-MS06-040 in order to spread swift and wide in large networks, targeting Windows 2000, XP and 2003 versions. According to Chinese agencies, the worm's proliferation seems to have been perpetrated by malware writers in Shanghai University, though it's now spilling out of the commercial capital of China, to spread fast in other Chinese cities as well.

As MicroWorld Technologies informed earlier, "Win32.IRCBot.st" is a PE executable packed with MEW. It appears as "wgareg.exe" in the Windows System folder with a description "Windows Genuine Advantage Registration Service". IRCBot.st uses the AOL Instant Messenger for its external mode of spreading routine.

Once inside the system, the Backdoor stops the computer's access to the Internet, changes Windows Security settings, turns off firewall and AntiVirus and connects to the remote attacker via IRC channels. In networks, this Backdoor sends out the exploit to infect vulnerable machines, explaining why so many users in China were affected in so less time.

“It’s ironic that ‘Win32.IRCBot.st’ has been invented to exploit an earlier vulnerability in Windows Plug-n-Play Service, tagged as MS05-039,” says Sunil Kripalani, Vice President, Global Sales and Marketing, MicroWorld Technologies. “Without much change in code, the Backdoor-worm now trains its guns on MS06-040. While our customers are well safeguarded against this worm, we strongly urge everyone to update their Windows systems with the latest security patches from Microsoft as there’s an imminent possibility of fresher exploits targeting the critical vulnerability.”

MS06-040 is a Server Service vulnerability that facilitates remote code execution in network computers, while the said Service listens on TCP ports 139 and 445. Now, one can effectively employ the ‘eConceal’ Firewall from MicroWorld Technologies to safeguard these ports and provide another layer of threat protection, reminds Sunil Kripalani.

Rated as Critical, MS06-040 has even prompted the US Homeland Security to issue a warning, while exploits are already out on the web. To download security patches for Windows, one can log on to

<http://www.microsoft.com/technet/security/bulletin/MS06-040.msp> .

## Company Profiles powered by ITReseller.com

- MicroWorld - [View profile](#)

---

[Links](#) | [About Us](#) | [Privacy Policy](#) | [Contact Us](#) | © 2004-2006 IT Backbones Limited

Site developed and hosted by [Design Solution](#) Ltd.