

IT BackbonesTM

Security News



An independent, non-profit organization
whose mission is to protect children
from potentially harmful material

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](#)

Backdoor Trojan Unleashes Dual-Media Attack

Published 28th June 2006

Security experts at MicroWorld Technologies have received reports about a text message being spammed to mobile phone users in US and parts of Canada, thanking them for subscribing to a nonexistent dating website that would charge them \$2 per day. To unsubscribe the service you are told to visit a URL and follow the instructions.

The professionally designed website directs you to click on a button that says 'unregister your mobile'. You are instructed to type in the mobile number in a textbox and click 'confirm' and subsequently a new window opens up telling you to run a program. The program is nothing but a deadly Backdoor Trojan named as Dumador.bc!

Dumador.bc is a Bot Trojan with keylogging capabilities. To connect to the remote attacker, it opens up dual TCP ports, communicating via 'GET' requests to multiple URLs. The Trojan also blocks websites of several AntiVirus firms by modifying the Windows 'HOSTS' file. The Keylogger component captures personal financial information pertaining to several leading banks and credit card companies, which are passed over to the malware author. Through the port, the attacker controls and manipulates the victim's computer to eventually turn it into a zombie.

"Our users updating their software have no reason to worry as we've been providing protection for this Trojan ever since Apr 11, 2005," informs Sulabh Mahant, Security analyst, MicroWorld Technologies. "What's intriguing here is the bi-layered mode of

proliferation with truly sophisticated Social Engineering. The thought of draining two dollars per day is good enough to make one panic. And the trick is all about inducing that state of mind where you lose senses and readily follow what the fraudster tells you to do”

Backdoor Trojans work surreptitiously in the background, while the infected user remains unaware of the hacker’s activities. Many a times they come bundled with popular games and utilities so as to arouse no suspicion what so ever. The person controlling the program can capture keystrokes, view files, steal screen shots and even work the mouse.

Botnets are created by grouping such infected computers, taken over by hackers using Backdoors and Trojans. These networks are employed in a plethora of illegal activities like Denial-of-Service attacks, hijacking SMTP Mail Servers to launch Spam campaigns, wrongfully increasing hit count of specific websites and proliferating deadly viruses.

MicroWorld Technologies produces the world’s most advanced Security Solutions with an R&D team that works 24*7. “This kind of an attack can hoodwink even the computer savvy and deliver the payload to the destination,” points out Govind Rammurthy, CEO, MicroWorld Technologies. “The only way to fight such tricky malware is to make sure that every piece of data coming into the computer is monitored with great vigil and Futuristic Security Intelligence. When it comes to fighting malware, your protective gear just can’t sit back and relax even for a fleeting moment!”

Company Profiles powered by ITReseller.com

- MicroWorld Technologies Inc - [View profile](#)

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

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