

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



Finjan gives you protection that signature-based products **cannot even see**

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

- [Home](#)
- [About](#)
- [Submit News](#)
- [Search News](#)
- [IT Events](#)
- [Time & Money](#)
- [European Media](#)

Have You Heard The New Buzz? It's MP3 Spam!

Published 24th October 2007

'Thou shalt try every new trick possible and thou shalt apply no discretion.'..

This looks like the new testament of the spammer fraternity. Proof to this is the new wave of Pump and Dump scam campaign sweeping across Europe and Unites States, which uses attached MP3 files touting the stock of a particular company, say Security Experts at the AntiVirus, AntiSpam and Content Security firm MicroWorld Technologies.

Some attachments are named after Elvis, Beatles, Carrie and Fergie in the typical Social Engineering style, while some others are named as oursong.mp3, dadsong.mp3, coolringtone.mp3 and listentothis.mp3. Once you download the file and play it, what you get to hear is a female voice speaking in British accent about the market prospects of a Canadian company!

"The quality of the sound file is kept poor in order to make it smaller in size, and it's not easy to understand what the spammer is trying to tell unless you try hard," says Manoj Mansukhani, Head - Global Marketing, MicroWorld. "It's quite unlikely that someone will get all fired up and run the next moment to buy the stock of the firm promoted in this spam. What I see is, in their bid to escape spam filters, spammers are trying out new file types with no discretion".

Men behind Pump and Dump campaigns buy shares of companies not doing well at cheap rates and soon start sending out millions of spam mails across the world to inflate their prices. The trick lies in the huge volume of mails and even if a negligible percentage of the recipients fall for the flimflam, the conmen's purpose will be served. As soon as the price of the stock goes up, they sell it off, making a fortune in the bargain.

“Checking the source of this campaign, we found that it's coming out of the Storm Trojan botnet, consisting of infected PCs owned by common people like you and me! And that makes it difficult for AntiSpam solutions that merely work on sender identification techniques like RBLs, which maintain a list of known spammers, to identify and block mails like these. That's why we at MicroWorld use a range of technologies in the spam filtering module of our products eScan and MailScan, while also providing options for completely blocking out file types like MP3 at the mail gateway if need be,” Manoj Mansukhani points out .

To filter spam, MicroWorld employs several technologies like MX/A DNS Record Verification, Reverse DNS, X-Spam Rules Check, Sender Policy Framework, RBLs and a revolutionary technology called Non Intrusive Learning Patterns. This self-learning and adaptive technology quickly recognizes and blocks new spam types like mp3 files.

On a broader perspective, spammers are here to stay and their equipments and targeted users are always expanding. To evade them, we need technologies that work intelligently and adaptively, so that however hard they try, they don't find a place in our mail boxes.

[Links](#) | [About Us](#) | [Privacy Policy](#) | © 2004-2007 IT Backbones Limited

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