



DEMAND PCI COMPLIANCE



Learn More >

- Flash Demo
- Free Trial
- Whitepaper

- ABOUT US
- CONTACT
- ADVERTISE

[Grab our main RSS feed and stay updated with fresh security news](#)

NEWS

- [Off The Wire](#)
- [Security](#)
- [World](#)
- [Virus Center](#)

ARTICLES

- [Latest Articles](#)
- [Reviews](#)
- [Interviews](#)
- [Book Chapters](#)

SOFTWARE

- [Windows Linux](#)
- [Mac OS X](#)
- [Pocket PC](#)

VULNERABILITIES

- [Vendor Advisories](#)
- [Vulnerability Database](#)

EVENTS

- [Webcasts](#)
- [Conferences](#)

NEWSLETTER

- [Subscribe](#)
- [Current Issue](#)
- [Archive](#)

HOME

E-MAIL ALERTS

SEARCH

RSS

OFF THE WIRE SECURITY WORLD

- [So many passwords, so little memory](#)
- [On your marks, get set, go: vulnerability mitigation race](#)
- [Q&A: Security top concern for new IETF chair](#)
- [Secure file deletion: fact or fiction?](#)
- [Most vote machines lose test to hackers](#)
- [Google plans YouTube antipiracy tool for September](#)
- [Inside threats: what's walking out your front door?](#)
- [New book: "Fuzzing: Brute Force Vulnerability Discovery"](#)
- [New book: "Network Warrior"](#)
- [Email spam attachments decreasing](#)
- [Uniloc security platform leverages power of Oracle Database 11g](#)
- [Threat Report: Record number of Web-borne attacks during 2007](#)

LATEST ARTICLES VIRUS CENTER

- [Guide to Online Antivirus Solutions: NanoScan and TotalScan](#)
- [Top 5 Security and Networking Widgets for Mac OS X](#)
- [Lock the Door and Make Sure Your Data is Protected](#)
- [The Rules for Computer Forensics](#)
- [How To Recover Forgotten Microsoft Word Passwords](#)
- [Spammed screensaver installs rootkits and trojan](#)
- [PayPal data stealing trojan and IcePack malware installer](#)
- [Malicious tool Icepack installs malware through exploits](#)
- [Microsoft Excel virus and a ransomware trojan](#)
- [Information on Pinch tool for creating custom Trojans](#)

SECURITY SOFTWARE



[++ GFI LANguard Network Security Scanner 8](#) • [Security System Analyzer 1.5.2](#) • [Password Policy Enforcer 5.0](#) • [WinSCP 4.0.3](#) • [Password Safe 3.09](#) • [Ad-Aware 2007 Free](#) • [Lavasoft Personal Firewall 2.0](#) • [SSL-Explorer 0.2.14.1](#) • [VisualRoute 2007 11.1a](#) • [J2SSH 0.2.9](#) • [JSch 0.1.33](#) • [Rootkit Hunter 1.3.0](#) • [Libnids 1.22](#) • [Shorewall 4.0.0](#) • [IPCop 1.4.16](#) • [Sussen 0.90](#) • [strongSwan 4.1.4](#) • [SILC Toolkit 1.1.2](#) • [GnuPG 2.0.5](#) • [Distributed Access Control System 1.4.19](#) • [Cyclone 1.0](#) • [pam\\_passwdqc 1.0.4](#) • [NuFw 2.2.2](#) • [NetShred X 4.0](#) • [TPM Setup 1.0](#) • [The DoorStop X Security Suite 2.0](#) • [LockMeBaby 1.12](#) • [1Passwd Password Manager 2.4.6](#) • [Shimo 1.0](#) • [Random Password Generator 1.6.1](#) • [Radmind Assistant 1.0.0](#) • [PDFKey Pro 3.4.1](#) • [MultiAlarm 3.4.2](#) • [Mac GPG 1.4.7](#) • [Little Snitch 1.2.4](#) • [SecuBox for Pocket PC 1.2](#) • [Crippin 2.12](#) • [Aircanner Mobile Encrypter 2.9](#) • [Sentry 2020 2.9](#) • [WiFiFoFum 2.1.1](#) • [AirFix 1.0b](#) • [Confidential Notes 1.1](#) • [Aircanner Mobile Firewall 2.4](#) • [WiFi Graph 0.3 RC3](#) • [SignWise Pro 2.52](#) • [eWallet 4.0](#) • [Pocket Warrior 15022003-B](#)



ADVISORIES



VULNERABILITIES

• [Slackware Security Advisory - bind \(SSA:2007-207-01\)](#) • [Mandriva Linux Security Update Advisory - clamav \(MDKSA-2007:150\)](#) • [Mandriva Linux Security Update Advisory - bind \(MDKSA-2007:149\)](#) • [Gentoo Linux Security Advisory - MIT Kerberos 5: Arbitrary remote code execution \(GLSA 200707-11\)](#) • [Gentoo Linux Security Advisory - Festival: Privilege elevation \(GLSA 200707-10\)](#) • [Debian Security Advisory - bind9 \(DSA 1341-1\)](#) • [STATCOUNTER.COM: Cross-Site Scripting and Cross-Site Request Forgery](#) • [Password exposure in Lotus Notes](#) • [Remote command execution in Joomla! CMS](#) • [CA Products Alert Service RPC Procedure Buffer Overflow Vulnerabilities](#) • [Multiple Vendor Multiple Product URI Handler Input Validation Vulnerability](#) • [Opera Software Opera Web Browser BitTorrent Dangling Pointer Vulnerability](#)

**GFI:** [Network & server monitoring made easy with GFI Network Server Monitor. FREE trial - download today!](#)

## Spam mails in PDF format flood the web

Posted on 18 July 2007.

If you thought emails carrying embedded images are the current trend in spam town, it's time to move on. According AntiVirus, AntiSpam and Content Security solution provider MicroWorld Technologies, the new in-thing is a deluge of PDF spam targeting your wallet.

MicroWorld experts have been intercepting large numbers of PDF spam doing rounds in the last two months, but their volumes surged dramatically since the beginning of July. Leading the pack are two 'Pump and Dump' Scams touting about some stocks in their bid to make you buy them.

The first one is about the stock of a German company called Talktech Telemedia. The well created PDF file looks like a leaf from a trade magazine with its neat design and business language. Like all Pump and Dump scams this one too tells you that, thanks to many positive factors happening in the next few weeks, the price of the stock in question will jump 300%. The second one is also stock related, albeit the PDF here is in a much basic and simpler form.

In Pump and Dump scandals, scamsters buy worthless shares of companies and send out spam mails across the world to drive up their prices. The total number of Talktech spam floating around is estimated to have crossed two billion so far.

A few people bite the bait and the buy the stock going by the 'confidential and profit making' opportunity! Once the stock price picks up, the people behind the scandal just sell their shares off to make huge profits while those who got sucked into the plot lose their hard earned money.

"Earlier, spammers used embedded images in mails to circumvent spam filters that work by checking for specific words and phrases in message content," says Govind Rammurthy, CEO of MicroWorld Technologies. "Many spam filters have now smartened up and they can identify and block such commercial mails. That's why the conmen behind these mass mails are trying out PDF file format to dwindle unsuspecting computer users".

"PDFs are traditionally used for drafting official documents and whitepapers. That's created an air of authenticity and authority about them which would make many drop their guard in downloading the attachment. The faulty perception that PDFs are immune to malware infections helps too," points out Govind Rammurthy.

PDF can carry viruses too as Govind indicates. A Worm named 'Worm.VBS.Peach' in 2001, was found to be propagating by using a PDF file as a carrier while it offered a puzzle game called 'Find the Peach' to the recipients. The Worm stole email addresses from the victim's address book and sent self copies to all email IDs found.

"Many spam filters are giving a slip to these mails while most computers now are equipped with Adobe Acrobat Reader which enables them to display PDF messages. These two factors mean that PDF spam is here to stay for sometime and spammers will continue to innovate in their bid to reach more mail boxes," concludes Govind Rammurthy.

[ [Security World main page](#) ]



VIDEO: THE STATE OF DATABASE SECURITY

Sponsored links:

[Home Security](#)

[Security software Australia](#)

[Security Cameras](#)

[Asset Tracking](#)

[Download KGB Keylogger!](#)

[Security systems](#)

[Security cameras](#)

[Security Camera Systems](#)

[Spy Equipment](#)

[Data Entry](#)

[Vulnerability Scanning](#)

[Network Vulnerabilities](#)

[Network Server Monitor](#)

[POS Software & Systems](#)

**GF*i*LANguard**  
Network Security Scanner

**Download Your  
FREE Trial Today!**

