

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



Give your mouse a heart!

search 

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

- **Home**
- **About**
- **Contact**
- **Submit News**
- **Search News**
- **What We Can Offer You**
- **IT Events**
- **Time & Money**

Trojan Dropper Fools Users With Infected Word File

Published 2nd November 2006

If you thought Macro Viruses are a thing of the past, think again!

AntiVirus experts at the world's most advanced IT Security Solution Provider, MicroWorld Technologies, advises computer users to apply caution while receiving Word files from unknown senders or when downloading them from untrusted websites. Infected documents may contain a Macro Trojan Dropper named MSWord.Lafool.v.

This Malware is a Macro that uses Microsoft Word's own programming language to advance its infection routine. Unlike most other Viruses, Macro Viruses do not infect programs, instead they target documents and templates. However, MSWord.Lafool.v acts differently, by working as a Trojan Dropper by exploiting a vulnerability in Word, in order to deposit an Information Stealing Trojan named PSW.LdPinch.bbg in victim's computer.

"One needs to view this variety along with the recent upsurge in Trojan Droppers that exploited MS office vulnerabilities including flaws in Microsoft Word. It might be interesting to note that most of these malware, spread with the help of vulnerability exploits, were dropping Password Stealing Trojans in the targeted computers," views Manoj Mansukhani, Head - Technology and Marketing, MicroWorld Technologies.

The dropped malware, PSW.LdPinch.bbg, is a data collecting Trojan with Backdoor capabilities. It can steal confidential data like FTP usernames and passwords, MS

Wallet passwords, networking information, RAS dial-up settings, Mail settings information and many more. In the hands of an intruder who targets confidential information of an organization, this Malware can be a highly effective tool for penetration and espionage.

“Knowledge is Money, figuratively and literally,” points out Govind Rammurthy, CEO, MicroWorld Technologies. “For a victim whose Credit Card information is stolen, it’s as good as his loaded wallet getting ripped off in broad day light. For an organization that loses its Knowledge Base and Intellectual Property, the damage could be well beyond some zeros vanishing in its bottom line. In this era of Knowledge Economy, organizations of every size and shape can afford to show no laxity in protecting their information systems and knowledge resources.”

MicroWorld Technologies proactively safeguards its users with eScan and MailScan, in order to insulate them against online threats like these by continuously updating their Detection System for latest Viruses, Trojans, Worms, Vulnerability Exploits other malware. The solutions also employ highly advanced Heuristic methods to tackle disguised and emerging threats, Govind Rammurthy adds.

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

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