

# IT Backbones<sup>TM</sup>

## 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](#)

## 'I love You' Mail Carries Bagle Worm In Zip File

Published 23rd June 2006

When you get an email from Anna, Alice or Ellyn saying that she loves you and offers you a password to open her heart, don't get carried away. The encrypted zipped file is a Bagle worm.

Security Analysts at MicroWorld Technologies inform that "Win32.Bagle.fy" comes via password protected ZIP archives attached to spammed emails with a variety of sender names and subject lines.

The subject of the mail is the name of a person chosen from a list that carries common ones like Alice, Andrew, Androw, Annes, Christean, Dorothy ,Edmond and many more. The mail body reads 'I love you' and shows an image of the randomly generated numeric password next to it. The worm employs its own SMTP engine to proliferate, spreading fast in US, Europe and South Asia when reports last came in.

"It's always a tendency of the human psyche to open up a protected secret and nobody knows it better than the Virus writer," said Govind Rammurthy, CEO, MicroWorld Technologies. "Now when you club that penchant with a message that says 'I love you', coming from a rather common name, the whole thing adds up to the temptation and smoothly gets you into its vicious design. This is smart Social Engineering with a heady mix of emotional ploys."

With its password protected encryption, 'Bagle.fy' evades detection by security

solutions at the Gateway provided by some popular AntiVirus firms. After finding an entry into the computer, the worm connects to many websites and downloads much more malicious stuff in the true tradition of Bagle family.

The Bagle family known for its innovation, fast mutation and adaptability has been hugely menacing and dangerous for enterprise security over last few years. These mass mailing worms coming in a wide variety of size, spite and modes of proliferation, have been advancing really fast into deadly Trojans that are even equipped with Rootkit capabilities. An earlier variant named Bagle.GE, carried a Rootkit component which hid the registry keys of another member, Bagle.GF.

“MicroWorld has always advocated for integrated security for enterprises with multi-tiered protection. Viruses and other malware need to be defeated at some point or the other before it sneaks into the user data. With our proactive technologies, gateway level protection and MWL technology, we leave nothing to chance in providing that layer after layer of protection,” reflected Govind Rammurthy.

## 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.