

# IT Backbones<sup>TM</sup>

## Security News



**INTERNET CONTENT  
RATING ASSOCIATION**

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**

## Insidious Network Worm Threatens Enterprise Security

Published 11th July 2006

If you are used to sharing data over the Internet or your enterprise's intranet, apply caution! A network worm that will eventually bring in dangerous Trojans to your computer, is on the prowl.

Security Analysts at MicroWorld Technologies inform that 'Win32.Detnat.a' is a Network worm that infects uncompressed PE (Portable Executable) files. With its unique algorithm and polymorphic nature, the worm employs a different mode of encryption each time it infects a file, while keeping the file size unchanged, making it hard to detect.

Detnat.a spreads on shared network resources and file sharing programs. At the second level of attack, the worm goes ahead and downloads 'Infostealer.Lineage', a Trojan that steals usernames and passwords of popular online game 'Lineage' and passes it on to the remote attacker. With its dynamic nature, Detnat can invite any other Trojan as well, if the writer of the worm decides so.

"One needs to be extremely careful while downloading executable attachments via emails or from the Internet," said Aneesh Paliwal, Security Analyst, MicroWorld Technologies. "A single infection in a workstation can proliferate wide in shared networks in no time and people using file sharing programs are particularly vulnerable to this mode of data corruption and theft."

Individual Users and subgroups can freely exchange files in the internal networks of most organizations. This makes it easier for the spreading routine of a worm like Detnat. If the worm stations itself in the startup folder of the workstation connected to a network, then it will come back every time when that computer reboots, even if one cleans up the entire network. In a more targeted operation, an attacker hitting the Server can ensure that every user logging on to that Server gets infected, pointed out Aneesh Paliwal .

In March, MicroWorld had reported about the Antinny worm which infects the Japanese file sharing program Winny. Top-secret military information, business documents of hundreds of corporate firms, confidential data of 'Liberal Democratic Party' and a thousand others were all floating over the Internet, creating an enormous flood of information leakage in Japan, thanks to Antinny.

"A large number of new and emerging Viruses and worms are targeting enterprises and their external and internal networks, to carry out a whole lot of nefarious activities," observed Govind Rammurthy, CEO, MicroWorld Technologies. "Often, malware creeps in through those vulnerabilities that we tend to overlook. One needs to safeguard the corporate email system, intranet and total Internet Access with great vigil as network infections can severely impact the Business Continuity of enterprises."

## 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.