

# IT Backbones<sup>TM</sup>

## Security News



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](#)

## Ransomware Virus Goes Ultra-Tech With RSA-330 Bit Encryption

Published 12th June 2006

You've heard about Trojans concatenating files or encrypting them using regular methods to create a hostage situation, and demand ransom to free the stolen data. This new Ransomware spreading wide and far in Russia, named GpCode.af, goes a step ahead and employs a 330 bit encryption algorithm from RSA to wreck havoc for infected users!

Security experts at MicroWorld Technologies inform that Ransomware named GpCode.af, spreads primarily via spammed emails written in Russian, hence the infection is by and large confined only to the former communist nation so far.

The mail posing to come from a UK marketing firm trying to setup shops in various cities of Russia, asks users to download an MS Word file to complete a job application process. Now, a job offer is an irresistible deal for many, in a nation where the economy is limping, while the jobs are shrinking. For sure, the smart Social Engineering ploy from the malware writer has hit the bull's eye, apparent in its large scale proliferation.

The attachment contains a 'Trojan Downloader'. Once inside the user computer, it logs on to a malicious website and brings in GpCode.af. The Ransomware goes ahead and encrypts a large variety of files with extensions created through permutations and combinations of three or four English alphabets, including:

doc, xls, pdf, zip, rtf, html and many more. After completing the high-end encryption from RSA, the attacker leaves a message in a file, readme.txt, and demands users to pay up for the decryption code in true gangster style. You are given an email id to find out the mode of payment.

“There are three important aspects to be noted in the case of GpCode.af,” points out Govind Rammurthy, CEO, MicroWorld Technologies. “First, the smart Social Engineering with emails offering employment opportunities. Second, its two-tier infection method with the use of spam and Trojan-Downloader. Third, the use of sophisticated RSA technology in data encryption and hijack. When you talk about malware evolution, they are evolving in code, supporting technology, extortion techniques, modes of proliferation and psychological ploys. It’s definitely a wholesome deal.”

Last week, MicroWorld had reported about MayArchive Trojan, which strings files together, archives them and directs victims to buy spurious online drugs worth \$75, for the access password.

“MicroWorld believes in Proactive Security for information systems. You can see that a small piece of malware coming in through an otherwise harmless Word file, quickly grows in threat levels and hijacks priceless information stored in your computer. This incident once again goes to prove that safeguarding every intrusion, big or small, holds the key to comprehensive Data Security,” says 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.