

<i>IT Management Begins With Security</i>		WebProWorld Security Forum		RSS	Subscribe to our RSS feed . Stay current with our latest!
	SecurityProNews	Breaking Security Related News Your Source for investigative security related reporting and breaking news			SPONSORED BY: McAfee <small>Proven Security™</small>
HOME	IT ARTICLES	NEWS	NEWSLETTER ARCHIVES	ABOUT US	ADVERTISE
SecurityProNews > News > Security News > Olympic Torch Hoax Burns A Hole In Productivity, Again			Search:		

[SecurityProNews > News > Security News > Olympic Torch Hoax Burns A Hole In Productivity, Again](#)

[[news_security_news](#)]

Olympic Torch Hoax Burns A Hole In Productivity, Again

Btv Raj
Contributing Writer
2006-09-14

[SecurityProNews: News RSS Feed](#)

[Security News RSS Feed](#)

[PRINT VERSION](#) [EMAIL](#) [BOOKMARK](#)

Olympic Torch Hoax Burns a Hole in Productivity, Again The Olympic Torch Virus Hoax is back in circulation in a big way.

This time it's seen doing rounds predominantly among Orkut Online Community members, informs Security Analysts at MicroWorld Technologies.

The hoax mail that appeared for the first time in the second week of February 2006, says you should never open an email with an attachment named "Invitation", regardless who sends it to you. Like a typical scare monger it screams that the Virus will burn the whole hard disk of your PC! In the pretext of educating you about its spreading routine, the hoax goes onto explaining how the entries in the address book of a victim are stolen and how the Virus starts mass mailing to those email addresses.

To lend some fabricated credibility to the hoax, the email quotes CNN, Microsoft and Security firms. The message ends with a strong plea to forward it to as many people as possible so that the humanity shall save their computer hard disks from massive destruction!

"The psychology behind hoax mails is an intriguing subject to delve into. For many, it's just the curiosity to see how fast and far these false mails travel, while they derive some sadistic pleasure watching its geometrical progression. Some chain mails are fraudulent, money-making tricks in the form of Ponzi Schemes and Multi-Level Marketing, where they just act as invitations to bigger troubles. And then there are absolutely malicious ones spreading false and harmful information among their

NetworkingFiles

McAfee TOTAL PROTECTION for Small Business No Payment Until September - [Click Here](#)

[Top Stories](#)

VIRUS WARNINGS

Newsletter Signup

Subscribe to SecurityProNews FREE!

[[more newsletters](#)]

Featured On:

AS FEATURED ON
NEWS NOW

article resources

Search Articles:

[[advanced search](#)]

WebProWorld.com

- **Get in-touch** with industry experts and leaders
- **Post** your site for review by expert and peers
- **Ask** Security, IT, Development and Design questions

Free Membership: [Join Now!](#)

Visit [WebProWorld.com](#)

recipients as well," analyzes Sulabh Mahant, Security Expert at MicroWorld Technologies.

There is a real, tangible cost to hoax mails. It will dent your Collective Productivity, occupy large Server spaces, choke bandwidth, clog mailboxes with unwanted stuff and spread totally misleading information in business communities. In year 2001, a false alarm was raised by a hoax mail saying that a Windows Utility file named 'sulfnbk.exe' with a funny looking icon, was a Virus and got countless victims to delete that useful OS component from their computers. If you see, the harm it did was no less than a Virus!

"Regular technologies used in Spam fighting like Real-time Black List, Reverse DNS or Gray Listing, will fall flat in front of hoax mails as here the sender is someone you know. Your spam fighting system should be smart enough to learn and apply an acquired Intelligence to spot and stop these mails from entering mail boxes. That's where our unique and patent pending technology called Non-Intrusive learning Patterns (NILP) succeeds in filtering Mail Traffic using a combination of Self-learning Capability and continuously updated, research based feeds from MicroWorld Server," points out Govind Rammurthy, CEO, MicroWorld Technologies.

MicroWorld

MicroWorld (www.mwti.net) is the developer of the world's first Real-Time Anti-Virus and Content Security software eScan for desktops and servers. Its communication security software, MailScan is the first comprehensive e-mail scanner for your SMTP/POP3 Mail Server.

MicroWorld Winsock Layer (MWL) is the revolutionary technology underlying these products, powering them to several certifications and awards by some of the most prestigious testing bodies, notable among them being Virus Bulletin, Checkmark, TUCOWS, Red Hat Ready, and Novell Ready. Combining their powerful scanner with MWL technology, MicroWorld solutions provide a Real-Time Proactive security for your systems. For network security of enterprises, eConceal Firewall is the latest powerful offering from MicroWorld.

Add to [Del.icio.us](#) | [Digg](#) | [Yahoo! My Web](#) | [Furl](#)

Get all the updates in RSS:

[*View All Articles by Btv Raj*](#)

About the Author:

To learn more, kindly visit <http://www.mwti.net>.

Olympic Torch Hoax Burns a Hole in Productivity Again

Btv Raj is the Content Writer and Creative Visualizer, MicroWorld Technologies.

[More news_security_news Articles](#)

SecurityProNews: News

RSS Feed

[Security News RSS Feed](#)



iEntry Featured Services: [Jayde Member Services](#) | [Forums](#) | [Freeware](#) | [Advertise with Us](#)

[Contact Us](#) | [Advertise](#) | [Newsletter Archive](#) | [Sitemap](#) | [Submit an Article](#) | [News Feeds](#)

SecurityProNews is an [iEntry, Inc.](#)® publication - 1998-2006 All Rights Reserved | [Privacy Policy](#) and

[Legal](#)

Join the WebProWorld Forums: [Click Here](#)