



Use and distribution of this article is subject to our [Publisher Guidelines](#) whereby the original author's information and copyright must be included.

Current Rating: Not rated

Instant Worm shows pictures of steamy model by *btv raj*

Users of the Instant Messaging and Internet Telephony software Skype, beware!

According to Security Firm MicroWorld Technologies, a Worm named Win32.Pykse.a is on the loose, spreading through an Instant Message that shows a skimpily clad picture of Sandra, a model, in return for installing the malware in their computers.

The link to the Worm comes as a message using the Skype API, chosen from a list of random links pointing to a jpg image hosted on Russian Websites. Then the tricky malware turns off the message alert feature in Skype so that a notification message will not be shown to the targeted user when he or she receives the malicious message.

As soon as the victim clicks the link, a Trojan Downloader is pushed into the computer, which goes ahead and brings in Pykse.a. Once inside the computer, the Worm attempts to connect to several websites, most of which are seemingly associated with click fraud scams.

Interesting enough, one site contains a legitimate content lifted from the 'Living Africa' website. Even better, another one looks like a counter website that monitors the number of computers the malware manages to infect. Then it starts sending out the malicious link to everybody in victim's contact list.

"By the look of it, this one seems like a pilot run of the attack as the malware author is checking the extent to which the Worm spreads. Next time, the attack can be more dangerous if the websites that the malware points to, contain more malicious code that forces its way to user computers by exploiting browser vulnerabilities or by offering allurements," observes Govind Rammurthy, CEO of MicroWorld Technologies.

Net Telephony and Instant Messaging are increasingly attracting the attention of Virus writers, as both are effective ways to spread malicious code in large numbers. Enterprise users and home users are at equal risk from threats of this nature and it just underscores the need for one and all to follow Secure Computing Practices, points out the Chief of MicroWorld.

MicroWorld Technologies makes eScan range of products which enable organizations to implement safe net usage practices across the board. With eScan, the usage of Instant Messenger and Web Access by employees can be managed and controlled at a central point, using Integrated Security Policies. This ensures that Worms and Trojans spreading via multiple vectors are tackled effectively from entering Enterprise networks.

As for home users, another target of Worms like these, MicroWorld provides protection with eScan Internet Security Suite. It tackles a range of malware like Virus, email Worm, IM Worm, Trojan, Rootkit, Spyware, Adware and more, while also delivering Spam Control and Content Security.

MicroWorld says users infected with Pykse.a can download MWAV toolkit or eScan trial version to clean up their computers. MicroWorld

MicroWorld Technologies (www.mwti.net) is the developer of highly advanced AntiVirus, Content Security and Firewall software solutions eScan, MailScan, and eConceal. MicroWorld Winsock Layer (MWL) is the revolutionary technology that powers most of MicroWorld products enabling them to achieve 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.

For more information, please visit www.mwti.net

About the Author

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

Click an icon to rate this article:

Bookmark this article:

 del.icio.us |  Furl |  Technorati |  Blinklist |  Reddit |  Spurl |  Everywhere Else

[ExactSeek](#) | [SiteProNews](#) | [Blog-Search](#) | [EzineHub](#) | [Best-SearchEngine](#) | [SEO-News](#) | [FreeWebSubmission](#)

Jayde Online, Inc. © Copyright 2007, All Rights Reserved.

JAYDE ONLINE
NETWORK