

Manish Katara
MicroWorld Technologies Inc.
Antivirus software with content
33045 Hamilton Court East, Suite 105
Framington Hills, Michigan
U.S 48334-338
Voice: +1-248-8489081
Fax: +1-248-8489085
E-Mail: manish@mwti.net
Website: [Visit Our Website](#)

Three-pronged Trojan attack threatens security on the Internet.

Two is company. Three is a crowd. If one is not enough, use two, if two is not enough, use three. This is the credo behind the co-ordinated Trojan threat looming on the horizon.

/24-7PressRelease/ - Framington Hills, MI, June 08, 2005 - If you thought you've seen everything there was to see of virus threats, think again. Experts are saying this is "unprecedented", and could be the next big one.

Glieder (Win32.Glieder.AK), Fantibag (Win32.Fantibag.A) and Mitglieder (Win32.Mitglieder.CT) are not names of a modern day version of The Three Musketeers. These are Trojans engineered for a hacker attack that will infect computers and open them for use in further attacks.

"Combating computer viruses is essentially a game of hide and seek," says Govind Rammurthy, CEO, MicroWorld Technologies, among the leading Security Solutions providers. "Hackers riding piggyback on viruses have only a short window of opportunity to maximize their gain before the viruses are detected, neutralized and logged into Virus Definition databases, 'vaccinating' the system against those strains.

Without continuing system vulnerability caused by virus infection there is little they can do to further their malicious ends like stealing personal information, credit card details and other sensitive and vital data. To achieve their ends they need to keep the system vulnerability going for more time. This co-ordinated Trojan threat is an attempt to the keep that 'backdoor' open, essentially buying time," he concludes.

Of the three, Glieder leads the initial charge. It sneaks past anti-virus protection to download and execute files from a long, hard-coded list of URLs and "plant" the infected machine with "hooks" for future use. On Windows 2000 and Windows XP machines, it attempts to stop and disable the Internet Connection Firewall and the Security Center service (introduced with Windows XP Service Pack 2). Then the Trojan accesses the URL list to download Fantibag. The way is now paved to launch the second stage of attack.

Sulabh, a tester with MicroWorld Technologies says of Fantibag, "Now Fantibag goes about attacking the networking feature of the infected system to prevent it from communicating with anti-virus firms and denying access to the Microsoft Windows Update site. It closes your escape route by making it impossible to download an anti-virus solution and any subsequent Windows security patch to your system. Effectively it helps Mitglieder (the third stage Trojan) open the 'backdoor' by shutting the other doors on you."

Mitglieder puts the system under complete control of the attacker by opening the 'backdoor' on a port using which the attacker can update the Trojan, to stay a step ahead of attempts to remove it, download and execute files, initiate an SMTP server to

relay spam, execute files on the infected computer and download and execute files via an URL. "This is what makes it scary," say Aarti, Assistant Manager, QA, MicroWorld Technologies. "The fact that the system can now be used as a remote controlled 'soldier' (bot) in an army (botnet) of similarly compromised machines to launch criminally motivated attacks, causing harm to Internet users."

Botnets thus formed can among other things, use your machine to launch Distributed Denial of service attacks which overload servers, making them crash, to send out spam, spread new Malware, plant Keylogger to retrieve your personal information like identity, passwords, account numbers etc., install Spyware, manipulate online polls/games, abuse programs like Google AdSense to cheat advertisers of revenue, and install Advertisement Addons for financial gain as in fake websites advertising services that don't exist.

"Botnets can even encompass over 50,000 host machines. The potential for mischief is huge," reflects Govind Rammurthy. "Such a three-pronged Trojan attack where attackers change their virus code and release viruses quickly to bypass virus signature scanners, then disable network access to deny the user link-ups to anti-virus and Microsoft Windows Update site for protection has huge significance for virus-signature based protection. It is a sign of things to come," he says, remembering the scramble at MicroWorld labs to update their products to detect and remove the three Trojans.

Anti-virus updates for the three-pronged Trojan threat are available at MicroWorld Technologies site.

Maybe the time for worrying about some pimply teenager turning out malicious code because they have nothing better to do on a nice sunny morning, is over. The world could be facing a determined organized crime syndicate who'll stop at nothing to get what they want - information precious to you.

For more information visit <http://www.mwti.net> or write to manish@mwti.net

About MicroWorld Technologies Inc.


MicroWorld Technologies Inc. is the publisher of world's first real time antivirus and content security software eScan and MailScan, for desktops and Mail Servers respectively. Headquartered in Michigan it has its development centre in India which Asia-Pacific and Europe headquarter. MicroWorld has presence in more that 74 countries today and reselling through a channel network of more than 13,000 Resellers, Distributors, Security partner and System Integrator.

MicroWorld's Revolutionary "MicroWorld-WinSock-Layer (MWL)" technology, the first of its kind in the world. It deals with these threats before they enter your network, in the same way that a firewall controls user access.

Our products, eScan and MailScan are reliable and time tested products and have been awarded some of the most prestigious awards and certificates in the internet security industry. These have been succesful in fighting the epidemics like SOBIG and the recent MyDoom attack.

VB 100%,
Checkmark,
Advanced CheckVir,
5 cows by TUCOWS,
Best content security and antivirus software -by VAR magazine

#

 Email this article to a friend

Need content for your website? Add our RSS or JavaScript Press Release Feeds

DISCLAIMER: For questions or concerns regarding legitimacy of news, please contact the company in question DIRECTLY. 24-7pressrelease.com is not responsible for the accuracy of the content posted on our site. Issuers of news are responsible in whole for content posted to our site.

Copyright 2004 24-7Press Release.com

[Terms of Service](#) | [Privacy Policy](#)

[Press Release Site Map](#)