



SELF SEO

Main Navigation

[Self SEO Home](#)

[Webmaster articles](#)

[Articles archive](#)

[Submit your article](#)

[Register](#)

[Login](#)

[Search](#)

[XML news feeds](#)

[Free RSS news reader](#) **NEW**

[Contact](#)

Webmaster tools

[Check Google Pagerank](#)

[Link Popularity Checker](#)

[Keyword Suggestion Tool](#)

[Search Engines Report](#)

[International WHOIS](#)

[What is my IP ?](#)

[IP to country](#)

[Find IP address of a website](#)

[Find host by IP](#)

Webmaster Articles

[Affiliate Marketing Articles](#)

[CGI Articles](#)

[Computer Related Articles](#)

[Copywriting Articles](#)

[Domain Name Articles](#)

[E-Books Articles](#)

[E Commerce Articles](#)

[Email Marketing Articles](#)

[Hardware Articles](#)

[HTML Articles](#)

[Internet Articles](#)

[Internet Connection Articles](#)

[Internet Marketing Articles](#)

[Javascript Articles](#)

[Link Popularity Articles](#)

Three pronged Trojan Attack Threatens Security on the Internet

Posted by By Manish Katara on: 2005-06-08 23:27:47

[Self SEO](#) > [Site Security Articles](#)

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

- [Newsletter Related Articles](#)
- [Online Auction Articles](#)
- [Online Promotion Articles](#)
- [Personal Tech Articles](#)
- [Podcasting Articles](#)
- [PPC Advertising Articles](#)
- [RSS Articles](#)
- [Search Engine Optimization Articles](#)
- [Search Engine Positioning Articles](#)
- [Search Engine Tactics Articles](#)
- [Software Articles](#)
- [Spam Related Articles](#)
- [Streaming Media Articles](#)
- [Traffic Analysis Articles](#)
- [Traffic Building Articles](#)
- [VoIP Articles](#)
- [Web Hosting Articles](#)
- [Web Design Articles](#)
- [Web Development Articles](#)
- [Webmaster Articles](#)
- [Website Security Articles](#)

Advertisement

A New Weapon For Your Arsenal

How blogs dramatically increase customer satisfaction.

RSSApplied.com



The SEO Book

Webmasters: I Guarantee I Can Triple Your Traffic - in 90 Days - or You Don't Pay A Single Penny!

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.

MicroWorld Technologies is one of the leading solution providers for Information Technology, Content Security and Communications Software. MicroWorld has established itself as a leader in providing content security, anti-virus and corporate communications software solutions.



Post New Comment

This site does not allow anonymous comments. Registered members can [login](#) to participate. [Registration](#) is free and takes only a few seconds

Copyright © selfseo.com

Powered by [Esselbach Storyteller CMS System](#) Version 1.7-Free