

WINDOWS

GAMES

DRIVERS

HANDHELD

MAC

LINUX

MOBILE

NEWS

Search:

+ BOOKMARK SOFTPEDIA

ADVANCED SEARCH >>

News area:

[Latest news](#)
[Softpedia Poll](#)
[Daily Gadget](#)
[Softpedia Opinions](#)
[News Categ.](#)
[Top News](#)
[TECHNOLOGY](#)
[SCIENCE](#)
[HEALTH](#)
[SPORTS](#)
[ENTERTAINMENT](#)
[BUSINESS](#)
[WORLD](#)
[EDITORIALS](#)
 Softpedia Reviews

Welcome!

Hello, Guest [Login](#) if you have a Softpedia.com account. Otherwise, [register](#) for one.

Trojan Bot Exploits Multiple Windows Vulnerabilities

 Category: [SOFTPEDIA NEWS](#) :: [Security](#) :: [Online Security](#)

And uses Win32.Rootkit.I to hide its files and processes and to avoid detection

By: Marius Oiaga, Technology News Editor



According to a security advisory published by MicroWorld Technologies, Backdoor.Rbot.ayg is a network based Trojan horse spreading via AOL Instant Messenger via Service Vulnerability-MS06-040

and previous vulnerabilities including MS03-049 in Windows. While the Redmond Company has released security bulletins addressing the vulnerabilities, unpatched systems extend the proliferation of Backdoor.Rbot.

“What’s worrying with these sorts of malware samples is that they show increased hybridization in code and Multiple Layering in mode of attack,” stated Manoj Mansukhani, Head-Technology and Marketing, MicroWorld Technologies. “This is a Backdoor Trojan with network creeping abilities, which uses a Rootkit component to hide itself. For spreading, it employs dual channels of Instant Messenger and Vulnerability Exploitation while the Rootkit deposited in the computer can even be used by a future Trojan. All this points towards a lot of planning, improvisation and innovation that goes into creating and proliferating malware today”

Moreover, MicroWorld Technologies has disclosed that the Backdoor.Rbot.ayg uses Win32.Rootkit.I to enable stealth files and processes and to avoid detection.

“If you are serious about security, you just can’t be complacent in patching vulnerabilities in Operating Systems or other applications. However, regardless of security flaws in OS or elsewhere, you must be able to rely on your

AntiVirus software to protect your system from all kinds of malware types,” advised Sunil Kripalani, Vice President, Global Sales and Marketing, MicroWorld Technologies. “And that will be possible only when the security software combines multiple technologies that are proactive and reactive in nature and always keeps a few steps ahead of Virus writers.”

RELATED LINKS

[Credit Card Email Drops Trojan](#)

[Samsung Telecom Website Hosting Malware](#)

[Basic Trojan Package for \\$20](#)

[Trojan Horse Dropped by Spoofed Email from Anti Child Pornography Organization](#)

[Sophos Reports August 2006 Malware Threats](#)

[Sophos Free Anti-Rootkit Detection and Removal Tool](#)

[15 Years in Prison for One Million Images of Child Pornography](#)

[Trojan Captures Data in Video Files](#)

Due to the avalanche of MMO titles being launched on the market, Softpedia would like to know your opinion about this ever increasing genre in the industry. Do you think it's going to reach a boiling point or is it going to become an integrant part of our lives? [Vote here!](#)

16th of September 2006, 11:54 GMT | Copyright (c) 2006 Softpedia | Contact: newseditor@softpedia.com

Rating: ★★★★★ | 0 vote(s) so far | Cast your vote:

Read by 331 user(s) | [Add comment](#) | [Link to this news](#)
 [Subscribe to news](#) |  [Print article](#) |  [Send to friend](#)

[Today's News](#) | [Yesterday's News](#) | [View News Archive](#)

Search:

TODAY'S HEADLINES: ● [The Stainless Steel Keyboard With Trackball](#) ● [Raven's Hollow Horror Adventure Title in Development at Hidden Sanctum](#) ● [Windows Vista Is Too Good to Be True](#) ● [Yahoo to Acquire Social Network Property](#)
● [Microsoft Downplays VLM Vulnerability](#) ● [Non-Microsoft Security Update for MSIE VML Vulnerability](#) ● [MSIE VML Exploits Cause SANS Internet Storm Center Code Yellow](#) ● [Microsoft Plans Ad Based Online MS Works](#)

 [Trojan Bot Exploits Multiple Windows Vulnerabilities - USER OPINIONS](#)

We are sorry, there are no opinions available for this article.

 [SHARE YOUR OPINION ABOUT Trojan Bot Exploits Multiple Windows Vulnerabilities](#)

Only registered and logged in users can post comments. Click here to [login](#), or [register](#).

 [DO YOU WANT TO CONTACT US?](#)

If you have some comments or you want to send us some information you can send us an email directly to newsen@softpedia.com. You can use the form below for the same purpose.

Your full name: (at least 3 characters)

Your email address: (at least 5 characters)

Message subject: (at least 5 characters)

Message text: (at least 10 characters)

© 2001 - 2006 Softpedia. All rights reserved.
Softpedia™ and Softpedia™ logo are registered trademarks of SoftNews NET SRL.

[Copyright Information](#) | [Privacy Policy](#) | [Terms of Use](#) | [Contact Softpedia](#) | [Update your software](#) | [Archive](#)