

For Immediate Release

For more information, contact:

Amelie Chauvel
AlphaShield Inc
604.435.0700
achauvel@alphashield.com

'Prevent Backdoor attacks from Fizzer with AlphaShield'

WHAT: A new worm has hit the Internet called Fizzer.

Fizzer is a mass-emailing virus that opens ports on your system and attempts to stop the software firewalls that are in operation. Fizzer is transferred via email with different subject or titles and through file sharing programs.

WHEN: First reports of Fizzer surfaced on May 8th, 2003

HOW: The worm is a file attachment with an extension .EXE, .PIF, .COM or .SCR. When the infected email is opened, Fizzer will copy itself to the Windows installation folder, and modify registry keys in order to launch every time a computer starts up and attaches to the shared files in a shared folder.

EFFECTS: Fizzer will try to spread itself by emailing to every address it finds in the Windows address book of the infected computer and through P2P (Peer to Peer) networks.

PREVENTING FIZZER ATTACKS WITH ALPHASHIELD:

AlphaShield will block portions of this virus that relate to hacking attacks, however the user will require an anti virus solution to 'stop' the virus. As AlphaShield is not an anti-virus solution, it will not 'stop' the virus if received via email or file sharing programs.

Fizzer has the ability to record all keystrokes on the keyboard and stores the information in a file it creates. Along with the capability to disable the firewall running on a system, Fizzer can also connect to AOL and IRC servers through a backdoor access point. Once the connection is made with the hacker, it can transmit all information retained and located, such as username, password of system and other keystrokes pressed by the user and where they were used.

This worm will open ports on a computer and wait for a remote incoming connection. Due to the fact that AlphaShield is a separate entity from the computer, it is unable to be affected by the Fizzer virus. Though the virus can open ports on the computer, with AlphaShield the Internet connection remains secure and inaccessible to the hacker. It cannot open any ports in AlphaShield. In order to do any damage onto a system, a hacker has to make the connection with the system. Since no port on AlphaShield is available for him to use, the security of the system can't be compromised.

The AlphaShield will prevent all emails from exiting the infected computer while in disconnect mode, either by timer or by pressing the grey (disconnect) button. However, AlphaShield is unable stop the mass emailing capability of Fizzer as it uses its SMTP engine to send emails from the infected system. Despite the fact that the user cannot stop the emailing, it is possible to monitor the AlphaShield to see if too much activity is going on between the system and the Internet by viewing the flickering lights on the front of the AlphaShield device. If there is too much activity, the user can activate the AlphaGAP technology by pressing the grey (disconnect) button and stopping all activity between the Internet and the computer, making all emails impossible to be sent as there will be no Internet available to the computer.

About AlphaShield

AlphaShield Inc. is the leading global provider of Internet security and privacy solutions ensuring data integrity, Internet and network privacy protection for today's consumers. AlphaShield is committed to setting a new standard for security integrity by providing consumers who utilize "always on" broadband Internet access with an easy-to-use, completely secure Internet privacy protection device. Founded in June 2000, AlphaShield is headquartered in Burnaby, BC. For more information, please visit www.alphashield.com.

###