More Bagle Variants Discovered as Virus Activity Increases

Submitted by: Write Angle Communications
Tuesday, 1 March 2005

Bagle.BM is latest in series of new variants discovered in a single day by AVG UK

Newark, UK, Mar 1, 2005 – AVG UK, the official business partner of Grisoft and the AVG Anti-Virus family of software products for the UK & Ireland, says Grisoft Labs today detected another new variation of the Bagle worm: Bagle.BM. This latest form of the Bagle computer virus joins the variants BB, BD and BE reported earlier today.

As with previous versions of the virus, Bagle.BM is spreading via the Internet as an attachment to infected email messages. Bagle.BM and today's other variants have a subtle difference. They do not spread themselves but are spammed en masse to email addresses previously acquired by spammers.

The Bagle.BM worm is a Windows executable file of 34KB. It is attached to messages which come with an empty subject. The body contains "new price" or just "price".

When a user opens the attachment it activates the worm which, in turn, launches the infected file. The worm then copies itself to the Windows system directory, and registers this file in the system registry. Bagle.BM also terminates processes designed to protect the victim machine and the local network. This leaves the infected machine vulnerable to further attacks by malicious code.

"The Bagle BM variant is one of several new strains seen by our labs this morning," says Michael Foreman, partner at AVG UK. "Users of AVG should be reassured that we have already issued an emergency update that will protect their systems from these latest threats.

"With several months since the last major outbreak, it looks like we may be entering a new period of increased virus activity," continued Foreman. "We are seeing an increase in the amount of malware sent by spammers. It has become the preferred method for expanding their network of infected machines used to deliver spam messages."

- ends -

About AVG Anti-Virus

AVG Anti-Virus software shields computers from viruses, trojans horses and worms with a multi-layer approach that is more comprehensive than most protection programs. Following extensive pre-processing to scan data for patterns of virus code, AVG moves on to examine files using generic detection to root out new strains or variants of known viruses. Two levels of heuristic analysis are performed – dynamic and static. The dynamic level uses code emulation to evaluate in a secure virtual environment the behaviour of the program or file being tested. Static heuristic analysis locates programming code associated with certain types of virus propagation. AVG then performs an integrity check. Certain data associated with each scanned file is stored in its internal integrity database and used to heal infected files, potentially restoring information, which may have been lost during infection. AVG supports all Windows operating systems, from Windows 95 through the latest version of Windows XP, and provides users with

extremely fast and efficient database updates to meet the latest viral threats.

About AVG UK

AVG UK, based in Newark, Notts is an innovator in value for network anti-virus solutions with sole responsibility for sales and marketing of the AVG Anti-Virus product family in the UK & Ireland. AVG UK provides advanced anti-virus software which is supported by one of the most accessible technical helpdesks in the industry. Its flagship product, AVG Network Edition, provides network anti-virus protection and management for SME networks. AVG Anti-Virus also supports SoHo, Professional, Email Server and Linux applications. The free version of AVG Anti-Virus provides a personal service for three million home users across the UK.

For further information please contact:

Michael Foreman
AVG UK
Tel: +44 (0)1636 700496
media@avguk.com

Paul Shlackman
Write Angle Communications
Tel: +44 (0)1276 683228
paul.shlackman@writeanglecomm.com