OTS0287 5 CA 0318 EUN0008 Di, 31.Mai 2005
International/Computer

H+BEDV warnt vor neuem Trojaner " TR/Dldr.Bagle.BR " mit dramatisch hoher Verbreitung

Tettnang (ots) - Die Antivirenspezialisten aus dem Hause H+BEDV Datentechnik warnen alle Anwender der Betriebssysteme Windows 95, Windows 98, Windows ME, Windows NT, Windows 2000, Windows XP sowie Windows Server 2003 vor dem Trojaner TR/Dldr.Bagle.BR. Der Trojaner verbreitet sich per Email und lädt weitere Trojaner-Komponenten nach. Das Schadens- und Verbreitungspotenzial dieser Bagle-Variante wird von den Virenexperten als äußerst hoch eingeschätzt. TR/Dldr.Bagle.BR wurde bereits im Vorfeld durch eine generische Signatur von der AntiVir-Heuristik erkannt.

TR/Dldr.Bagle.BR hat eine Größe von 36.352 Bytes. Er besitzt, wie auch seine Vorgänger, eine eigene SMTP Engine. Als SMTP Engine bezeichnen Antivirenhersteller ein Programm, das selbständig Emails verschicken kann.

Wird der TR/Dldr.Bagle.BR ausgeführt, erstellt er im Windows Systemverzeichnis (Unter Microsoft Windows 9x unter %WinDIR%System und mit Microsoft Windows NT/2000/XP/2003 unter %WinDIR%System32) zwei unterschiedliche EXE-Dateien und legt zwei Einträge in der Windows Registry an. Eine davon, die Datei WIWSHOST.EXE, ist der eigentliche Downloader. Er ist in der Lage, die Lauffähigkeit von Antiviren- und Sicherheitssoftware zu beeinflussen. Hierzu beendet er alle aktiven Prozesse, die eine der folgenden Zeichenkette im Prozessnamen enthalten.

Außerdem modifiziert er die Windows HOSTS Datei so, dass Webseiten von solchen Softwareherstellern geblockt werden und somit nicht mehr erreichbar sind.Ebenfalls ist der Trojaner in der Lage, verschiedene System-Services zu beenden. Sollten entsprechende Einträge vorhanden sein, löscht TR/Dldr.Bagle diese aus der Windows Registry. Der Trojaner enthält eine Liste mit URL's, von denen er weitere Komponenten nachladen kann und diese im Windows Verzeichnis mit unterschiedlichem Namen speichert. Die Liste der URL's unterscheidet sich von Variante zu Variante.

Das AntiVir Update ist auf der H+BEDV Webseite frei verfügbar.

Auch Privatanwender können sich effektiv gegen den ungebetenen

Besucher schützen. Die neue AntiVir PersonalEdition Premium unter www.antivir-pe.de bietet umfassenden Schutz für den heimischen PC.

Rückfragehinweis:

H+BEDV Datentechnik GmbH
Karin Klösges
Lindauer Strasse 21
D-88069 Tettnang
Tel.: +49 (0) 7542 - 500 0
Fax: +49 (0) 7542 - 525 10
Email: presse@antivir.de
www.antivir.de

OTS0287 2005-05-31/19:32

311932 Mai 05

Link zur Aussendung:
http://www.ots.at/presseaussendung/OTS_20050531_OTS0287