March 13, 2003

U.S. Department of Justice
United States Attorney
Western District of Missouri
Todd P. Graves
400 East Ninth Street, Room 5510
Kansas City, MO 64106
Contact: Don Ledford
Public Affairs
Phone: (816) 426-4220

St. Joseph Man Pleads Guilty in District's First Computer Hacking Conviction

KANSAS CITY, Mo. - Todd P. Graves, United States Attorney for the Western District of Missouri, announced today that a St. Joseph man pleaded guilty in federal court today to unauthorized computer intrusion. Graves noted that this is the first conviction for computer hacking prosecuted by the district's new Computer Crimes and Child Exploitation Unit. Richard W. Gerhardt, 43, of St. Joseph, Mo., pleaded guilty before U.S. District Judge to an indictment returned by a federal grand jury on Dec. 19, 2002. By pleading guilty, Graves said, Gerhardt admitted that he gained unauthorized access to the network computer system of Nestle USA while employed as an information systems consultant, working primarily at the Friskies Petcare plant in St. Joseph. Friskies Petcare is a corporate subsidiary of Nestle USA, which in turn is a subsidiary of Nestle S.A. of Vevey, Switzerland.

"Most of the work of the Computer Crimes and Child Exploitation Unit has been focused on child pornography and Internet-related exploitation of children," Graves said. "The successful prosecution of the district's first computer hacking case is a public reminder that our office remains committed to prosecuting all computer-related crime." Gerhardt's hacking activity, Graves said, resulted in a loss to Nestle USA of about $10,000. Under the terms of today's plea agreement, Gerhardt would pay that amount in restitution to the company. With the growth of the Internet and the widespread use of computer technology, Graves said, law enforcement officials must be equipped to meet new challenges. "We now have the resources and the tools in hand to combat high-tech criminals," he said. "There is no safe refuge in cyberspace, whether for child pornographers or Internet swindlers or, as in this case, computer hackers." The United States Attorney's Office for the Western District of Missouri gained additional funding last year for prosecutors and support staff for the new Computer Crimes and Child Exploitation Unit. The Western District of Missouri is one of only 13 districts in the nation to receive federal funding for such a unit, which includes a new computer forensics analyst. This analyst, Graves explained, will work closely with the FBI's Heart of America Regional Computer Forensic Laboratory (one of only five such facilities in the nation). Under the terms of today's plea agreement, Gerhardt also agreed to perform 250 hours of community service, either during a term of supervised release following a prison sentence or as a condition of probation, by speaking to public groups, advising them of the dangers associated with computer hacking, and publicly discouraging others from engaging in computer hacking conduct by warning them that those who engage in such conduct can suffer a federal felony conviction. On five separate occasions between August 12,

2001, and June 10, 2002, Gerhardt gained access to the Nestle network computer system without authorization and in excess of his authorized access, Graves said. Gerhardt admitted to downloading approximately 5,000 user account passwords from Nestle's system, which forced the firm to conduct a damage assessment of, verify the security of, and restore the integrity of its computer system. The various offices and facilities of Nestle USA and Nestle S.A. throughout the United States and the world, including the Friskies Petcare plant in St. Joseph, are linked together by a network computer system. Any computer or server connected to that system, Graves explained, is thus a "protected computer" under federal law. Gerhardt used a password-cracking software called "L0phtCrack" to retrieve the passwords for user accounts on the system. Gerhardt then created a database containing the user account passwords, Graves said, and stored the database in a file on a computer server connected to the system and in a file located on a laptop computer issued to him by Nestle.

Gerhardt admitted that he ran at least one password recovery utility program while on the system, then stored the results in at least one .zip file, creating a file which contained passwords he had obtained. Without authorization, Graves said, Gerhardt loaded and installed a program called "pwdump.exe" on the Nestle network computer system and on the laptop computer issued to him by Nestle. The "pwdump.exe" program is associated with an automated command that, at a preset time each day, communicated to other computers on the Nestle network computer system and downloaded active accounts and passwords. Gerhardt admitted that, on June 3, 2002, he caused the output from the "pwdump.exe" program to be stored on a computer server connected to the Nestle computer network system. Approximately 5,000 passwords associated with users of the Nestle computer network system were accessed and stored by Gerhardt.

On June 4, 2002, Gerhardt used a dial-up connection to log onto the Nestle network computer system from a remote location. While on the system, Gerhardt created a new and unauthorized administrator account. As a result of today's guilty plea, Gerhardt may be subject to a sentence of up to five years in federal prison without parole, plus a fine up to $250,000. The case is being prosecuted by Assistant U.S. Attorney Gene Porter. The case was investigated by the Federal Bureau of Investigation.

###