NEWS RELEASE

Thomas P. O'Brien
United States Attorney
Central District of California

Thom Mrozek, Public Affairs Officer
(213) 894-6947
thom.mrozek@usdoj.gov
www.usdoj.gov/usao/cac

For Immediate Distribution

November 9, 2007

COMPUTER SECURITY CONSULTANT CHARGED WITH INFECTING UP TO A QUARTER MILLION COMPUTERS THAT WERE USED TO WIRETAP, ENGAGE IN IDENTITY THEFT, DEFRAUD BANKS

In the first prosecution of its kind in the nation, a well-known member of the "botnet underground" was charged today with using "botnets" – armies of compromised computers – to steal the identities of victims across the country by extracting information from their personal computers and wiretapping their communications.

John Schiefer, 26, of Los Angeles (90011), has agreed to plead guilty to four felony counts: accessing protected computers to conduct fraud, disclosing illegally intercepted electronic communications, wire fraud and bank fraud.

The criminal information and plea agreement filed this morning in United States District Court in Los Angeles outline a series of schemes in which Schiefer and several associates developed malicious computer code and distributed that code to vulnerable computers. Schiefer and the others used the illicitly installed code to assemble armies of up to 250,000 infected computers, which they used to engage in a variety of identity theft schemes. Schiefer also used the compromised computers to defraud a Dutch advertising company.

In his plea agreement, Schiefer acknowledged installing malicious computer code, or "malware," that acted as a wiretap on compromised computers. Because the users of those compromised computers were unaware that their computers had

been turned into " zombies," they continued to use their computers to engage in commercial activities. Schiefer used the malware, which he called a " spybot," to intercept electronic communications being sent over the Internet from those zombie computers to www.paypal.com and other websites. Once in possession of those intercepted communications, Schiefer and the others sifted through the data to mine usernames and passwords. With Paypal usernames and passwords, Schiefer and the others accessed bank accounts to make purchases without the consent of the true owners. Schiefer also acknowledged in the plea agreement that he transferred both the wiretapped communications and the stolen Paypal information to others. It is the first time in the nation that someone has been charged under the federal wiretap statute for conduct related to botnets.

In another scheme, Schiefer installed malware on zombie computers running Microsoft operating systems, causing them to disgorge usernames and passwords from a secure storage area known as the PStore. Schiefer and his co-schemers caused the zombie computers to send that account access information to computers that Schiefer and his co-schemers controlled. Once again, Schiefer located Paypal usernames and passwords among this data and used that authentication information to access victim bank accounts.

Finally, Schiefer acknowledged defrauding an Internet advertising company with his botnets. Schiefer signed up as a consultant with a Dutch Internet advertising company and promised to install the company' s programs on computers only when the owners gave consent. Instead, Schiefer and two co-schemers installed that program on approximately 150,000 computers that were infected with their malware. To avoid detection by the advertising company, Schiefer instructed his associates to moderate the number of installations so it appeared that the installations were legitimate and not the result of a malicious computer program that was propagating itself. Schiefer was ultimately paid more than $19,128.35 by the advertising company.

Schiefer has agreed to make an initial appearance in Los Angeles on November 28 and to be arraigned on December 3.

Once he pleads guilty to the four counts, Schiefer will face a statutory maximum sentence of 60 years in federal prison and a fine of $1.75 million.

This case was investigated by the Federal Bureau of Investigation.

CONTACT: Assistant United States Attorney Mark C. Krause
Cybercrime and Intellectual Property Section
(213) 894-3493

Release No. 07-143