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

April 16, 2008

INFORMATION SECURITY CONSULTANT PLEADS GUILTY TO FEDERAL WIRETAPPING AND IDENTITY THEFT CHARGES

In the first prosecution of its kind in the nation, a man who is well known to members of the "botnet underground" pleaded guilty today to federal charges related to his use of "botnets" – armies of compromised computers – to steal the identities of victims throughout the country by extracting information from their personal computers and wiretapping their communications.

John Schiefer, 26, of Los Angeles (90011), appeared today before United States District Judge A. Howard Matz and pleaded guilty to accessing protected computers to conduct fraud, disclosing illegally intercepted electronic communications, wire fraud and bank fraud.

During today's court hearing, Schiefer admitted that he gained access without authorization to hundreds of thousands of computers in the United States and that he remotely controlled these compromised machines through computer servers. Once in control of the "zombie" computers, Schiefer used his botnets to search for vulnerabilities in other computers, intercept electronic communications and engage in identity theft.

"While computer criminals have many technological resources at their disposal, we have our own technology experts, as well as a host of legal remedies to punish those who exploit the Internet for nefarious purposes," said United States Attorney Thomas P. O'Brien. "As Internet-based criminals develop new

techniques, we quickly respond to their threats and prosecute those who compromise our ability to safely use the Internet."

In connection with the wiretapping scheme, Schiefer admitted that he and others installed malicious computer code, known as "malware," on zombie computers that captured electronic communications as they were sent from users' computers. Because victims with compromised computers did not know that their computers had become infected and were "bots," they continued to use their computers to engage in commercial activities, such as making online purchases. Schiefer's "spybot" malware allowed him to intercept communications sent between victims' computers and financial institutions, such as PayPal. Schiefer sifted through those intercepted communications and mined usernames and passwords to accounts. Using the stolen usernames and passwords, Schiefer made purchases and transferred funds without the consent of the victims. Schiefer also gave the stolen usernames and passwords, as well as the wiretapped communications, to others. Schiefer is the first person in the nation to plead guilty to wiretapping charges in connection with the use of botnets.

Schiefer also admitted stealing information from numerous computers by accessing the PStore, which is intended to be a secure storage area of computers running Microsoft operating systems. To accomplish this, Schiefer installed malware on computers that caused them to send account access information, including usernames and passwords for PayPal and other financial websites, to computers controlled by Schiefer and his co-schemers. Schiefer used that information to make unauthorized purchases using funds transferred directly from victims' bank accounts. Schiefer is the first known defendant to plead guilty botnets to harvest information from the PStores.

Finally, Schiefer admitted defrauding a Dutch Internet advertising company with his armies of zombie computers. Schiefer signed up as a consultant with the advertising company and promised to install the company's programs on computers only when the owners of those computers gave consent. Instead, Schiefer and two co-schemers installed that program on approximately 150,000

zombie computers whose owners did not give consent. Schiefer was ultimately paid more than $19,000 by the advertising company.

In addition to his guilty pleas to the criminal charges, Schiefer has agreed to pay approximately $20,000 in restitution to the Dutch advertising company and financial institutions that he defrauded.

“ Los Angeles has been on the front lines in the war against botnet herders and those who utilize their product," said Salvador Hernandez, Assistant Director in Charge of the FBI in Los Angeles. "As demonstrated by the Schiefer investigation, criminals increasingly use computers to facilitate a variety of illegal activities. As technology advances, so do the techniques engineers of cybercrime use to exploit the vulnerabilities of computer systems and users. Through the use of cutting edge techniques, the FBI is meeting the evolving threats in cyberspace by identifying and building cases on the worst offenders. This case should send a message to would-be cyber culprits that the FBI may be only a few mouse clicks away from finding you.”

Schiefer, who used the online handle “ acidstorm,” is scheduled to be sentenced by Judge Matz on August 20. At that time, he faces 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
Cyber and Intellectual Property Crimes Section
(213) 894-3493

Release No. 08-042