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

March 4, 2009

INFORMATION SECURITY CONSULTANT SENTENCED TO 4 YEARS IN PRISON IN FEDERAL WIRETAPPING AND IDENTITY THEFT CASE

Concluding the first prosecution of its kind in the nation, a man associated with the "botnet underground" was sentenced late today to 48 months in federal prison for using his "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, 27, of Los Angeles, who used the online handle "acidstorm," pleaded guilty last year to accessing protected computers to conduct fraud, disclosing illegally intercepted electronic communications, wire fraud and bank fraud. Schiefer was sentenced by United States District Judge A. Howard Matz, who also ordered the defendant to pay a $2,500 fine.

When he pleaded guilty, Schiefer admitted that he illegally accessed 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.

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 others. Schiefer used that information to make unauthorized purchases using funds transferred directly from victims' bank accounts.

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.

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. 09-022