NEWS RELEASE

For Immediate Distribution

February 11, 2008

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

YOUNG 'BOTHERDER' PLEADS GUILTY TO INFECTING MILITARY COMPUTERS AND FRAUDULENTLY INSTALLING ADWARE

A well-known juvenile member of the "botnet underground" pleaded guilty this afternoon to delinquency charges related to his use of "botnets" – armies of compromised computers – to surreptitiously install adware on computers, including military computers.

A male juvenile – who in court papers is identified as B.D.H., and who used the online nickname "Sobe" – appeared today before United States District Judge Manuel L. Real and entered guilty pleas to two counts of juvenile delinquency. The charges relate to B.D.H. conspiring to commit wire fraud, causing damage to computers used by the federal government in national defense, and accessing protected computers without authorization to commit fraud.

During the court hearing, B.D.H. admitted to participating in a scheme with Jeanson James Ancheta to gain unauthorized access to hundreds of thousands of computers in the United States, which they controlled remotely through computer servers. Specifically, B.D.H. and Ancheta would transmit malicious code over the Internet to scan for and exploit vulnerable computers. During the course of the scheme, B.D.H. infected computers belonging to the Defense Information Security Agency. He also claimed to infect computers belonging to Sandia National Laboratories.

Once in control of those "zombie" computers, B.D.H. and Ancheta would

cause the infected computers to be directed to computer servers that they controlled where they could install adware on the infected computers. The adware had been previously modified so that it could be surreptitiously installed on the zombie computers without the knowledge of the owners of those computers. Once the adware was installed, Ancheta would demand payment from each of the Internet advertising companies for each fraudulent installation of their adware. Ancheta would then pay B.D.H. a portion of each payment he received from those companies.

B.D.H. and Ancheta were able to avoid detection by network administrators, security analysts and law enforcement by varying the download times and rates of adware installations and by using different servers. B.D.H. and Ancheta also would discuss temporarily shutting down their operations in response to enforcement efforts by the Federal Bureau of Investigation.

B.D.H. is scheduled to be sentenced by Judge Real on May 5. At sentencing, the defendant faces a statutory maximum sentence of 15 years in custody, although juvenile defendants can be incarcerated only until they turn 21. The plea agreement in the case contemplates a prison sentence of one year to 18 months.

Ancheta is currently in federal prison after pleading guilty, see: http://www.usdoj.gov/usao/cac/pressroom/pr2006/051.html).

This case was investigated by the Federal Bureau of Investigation, which received assistance from the Southwest Field Office for the Naval Criminal Investigative Service and the Western Field Office of the Defense Criminal Investigative Service.

CONTACT: Assistant United States Attorney Mark C. Krause
(213) 894-3493

Release No. 08-013