



## **NEWS RELEASE**

**Debra Wong Yang**  
United States Attorney  
Central District of California

---

For Immediate Distribution

January 23, 2006

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

### **BOT HERDER PLEADS GUILTY TO FRAUDULENT ADWARE INSTALLS AND SELLING ZOMBIES TO HACKERS AND SPAMMERS**

In the first prosecution of its kind in the nation, a well-known member of the “botmaster underground” pleaded guilty this morning to federal charges related to his profitable use of “botnets” – armies of compromised computers – which were used to launch destructive attacks, to send huge quantities of spam across the Internet and to receive surreptitious installations of adware.

Jeanson James Ancheta, 20, of Downey, California, appeared today before United States District Judge R. Gary Klausner and entered guilty pleas to charges of conspiring to violate the Computer Fraud Abuse Act, conspiring to violate the CAN-SPAM Act, 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, Ancheta admitted using computer servers he controlled to transmit malicious code over the Internet to scan for and exploit vulnerable computers. Ancheta caused thousands of the compromised computers to be directed to a channel in Internet Relay Chat which he controlled, to scan for other computers vulnerable to similar infection, and to remain “zombies” vulnerable to further unauthorized accesses.

Ancheta further admitted that, in more than 30 separate transactions, he earned approximately \$3,000 by selling access to his botnets to other computer users for the purpose of launching distributed denial of service (DDOS) attacks and sending unsolicited commercial email, which is commonly called spam. Ancheta acknowledged specifically discussing with those who leased his botnets the nature and extent of the DDOS attacks or proxy spamming they were interested in conducting. Ancheta suggested the number of bots or proxies they would need to accomplish the specified acts, tested the botnets with them to ensure that the DDOS attacks or proxy spamming were successfully carried out, and advised them on how to properly maintain, update and strengthen their purchased armies.

In relation to the computer fraud count, Ancheta admitted generating roughly \$60,000 in advertising affiliate proceeds by directing more than 400,000 infected computers that were part of his botnet armies to other computer servers he controlled where adware he had modified would surreptitiously download onto the zombies. By varying the download times and rates of the adware installations, as well as by redirecting the compromised computers between various servers equipped to install different types of modified adware, Ancheta avoided detection by the advertising affiliate companies who paid him for every install. Ancheta further admitted using the advertising affiliate proceeds he earned to pay for, among other things, the multiple servers he used to conduct his illegal activity.

In addition to his guilty pleas to the criminal charges, Ancheta agreed to pay roughly \$15,000 in restitution to the Weapons Division of the United States Naval Air Warfare Center in China Lake and the Defense Information Systems Agency, whose national defense networks were intentionally damaged by Ancheta's malicious code. Ancheta also stipulated to the forfeiture of all of the proceeds of his illegal activity, including more than \$60,000 in cash, a BMW automobile and

computer equipment.

Ancheta is scheduled to be sentenced by Judge Klausner on May 1. At sentencing, the defendant faces a statutory maximum sentence of 25 years in prison.

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

CONTACT: Assistant United States Attorney James M. Aquilina  
(213) 894-6875

Release No. 06-007