U.S. Department of Justice

Debra Wong Yang
United States Attorney
Central District of California

United States Courthouse
312 North Spring Street
Los Angeles, California 90012

PRESS RELEASE

FOR IMMEDIATE RELEASE
November 3, 2005

For Information, Contact Public Affairs
Thom Mrozek (213) 894-6947

COMPUTER VIRUS BROKER ARRESTED FOR SELLING ARMIES OF INFECTED COMPUTERS TO HACKERS AND SPAMMERS

Indictment also Alleges Scheme to Use Botnets to Install Adware for Profit

Botnet Indictment

Los Angeles, CA - In the first prosecution of its kind in the nation, a well-known member of the "botmaster underground" has been indicted on federal charges for profiting from the use of "botnets" – armies of computers that are under the control of the botmaster and are used to launch destructive attacks or to send huge quantities of spam across the Internet.

Jeanson James Ancheta, 20, of Downey, California, was arrested this morning by special agents with the Federal Bureau of Investigation. Ancheta was indicted yesterday in two separate conspiracies, as well as substantive charges of attempting to cause damage to protected computers, causing damage to computers used by the federal government in national defense, accessing protected computers without authorization to commit fraud and money laundering.

The 17-count indictment alleges that Ancheta wrote malicious computer code, spread that code to assemble armies of infected computers, and sold access to the infected computers for the purpose of launching distributed denial of service (DDOS) attacks and sending spam. Ancheta also allegedly used the botnets to generate income from the surreptitious installation of adware on the infected computers.

The first conspiracy alleged in the indictment accuses Ancheta of modifying and disseminating the Trojan horse program "rxbot," which allowed him to create botnets, each with thousands of Internet-connected computers reporting to an Internet Relay Chat (IRC) channel that Ancheta controlled. In a separate IRC channel, Ancheta advertised the sale of his botnets to those interested in launching DDOS attacks or distributing spam without detection.

After receiving payment from customers, according to the indictment, Ancheta would give customers control of enough botnets to accomplish their specified task. Ancheta would also provide an instructional manual that included the commands needed to instruct the botnets to launch DDOS attacks or send spam. The manual would also

include the malicious code that would allow the botnets to spread or propagate. As part of his fee, Ancheta allegedly set up and tested the purchased botnet to ensure that the DDOS attacks or spamming could be successfully carried out.

The second conspiracy outlined in the indictment alleges that Ancheta caused adware to be downloaded onto the infected computers that were part of his botnet armies. To do this, Ancheta allegedly directed the compromised computers to other computer servers he controlled where adware he had modified would surreptitiously install onto the infected computers.

Ancheta had become an affiliate of several different advertising service companies, and those companies paid him a commission based upon the number of installations. To avoid detection by network administrators, security analysts and law enforcement, Ancheta would vary the download times and rates of the adware installations. When companies hosting Ancheta's adware servers discovered the malicious activity, Ancheta redirected his botnet armies to a different server he controlled to pick up adware. To generate the roughly $60,000 he received in advertising affiliate proceeds, Ancheta caused the surreptitious installation of adware on approximately 400,000 compromised computers. Ancheta used the advertising affiliate proceeds he earned to pay for, among other things, the multiple servers used to conduct his schemes.

Ancheta used programs powerful enough to cause the infection of computers at the Weapons Division of the United States Naval Air Warfare Center in China Lake, as well as computers belonging to the Defense Information Systems Agency, a component of the United States Department of Defense. Both networks are used exclusively by the federal government in furtherance of national defense.

After being arrested this morning at the FBI Field Office in Los Angeles, Ancheta was transported to United States District Court in Los Angeles. It is unclear if he will make his initial court appearance this afternoon or tomorrow.

Ancheta is charged with two counts of conspiracy, two counts of attempted transmission of code to a protected computer, two counts of transmission of code to a government computer, five counts of accessing a protected computer to commit fraud and five counts of money laundering. Count 17 of the indictment seeks the forfeiture of more than $60,000 in cash, a BMW automobile and computer equipment that the indictment alleges are the proceeds and instrumentalities of Ancheta's illegal activity.

If convicted of all charges in the indictment, Ancheta faces a statutory maximum sentence of 50 years in prison.

An indictment contains allegations that a defendant has committed a crime. Every defendant is presumed innocent until and unless proven guilty.

This case was investigated by the FBI in Los Angeles with the assistance of the Southwest Field Office of the Naval Criminal Investigative Service and the Western Field Office of the Defense Criminal Investigative Service.

#####

Release No. 05-148