Techie Pleads Guilty to Highjacking Computers

Source: USA Today, JAN 24, 2006

In the first case of its kind, a 20-year-old California man pleaded guilty Monday to hijacking hundreds of thousands of computers and selling access to others to spread spam and launch web attacks.

Jeanson James Ancheta of Downey, Calif., admitted to felony charges for breaking into military computers and for selling access to groups of hijacked PCs called bot nets.

Security experts say bot nets have increased dramatically in the past two years, partly driven by a wave of relatively unsophisticated "bot herders" like Ancheta, who tap into tools and instructions widely available on the Internet.

Computer-security giant Symantec says it has been tracking communications between more than 10,000 hijacked PCs per day in the first six months of 2005 -- double what it saw in December 2004. McAfee, another security firm, detected 32,000 distinct bot networks last year, triple that in 2004.

Those numbers probably understate the actual level of activity, since bots "conceal their controller," says Fred Felman, analyst at tech security firm Tenebril. Security experts say elite bot herders go to great lengths to stay hidden, and sometimes raid each others' networks.

"The market has gotten so crowded they're actually fighting for real estate on these compromised PCs," says Charles Renert, security research director for security-software supplier Determina.

Ancheta's activities over 14 months dating back to June 2004 were rudimentary, security experts say. He modified a widely available hijacking program, called rxbot, to usurp control of as many as 700,000 PCs. He earned about $60,000 using bot nets to distribute adware -- advertisements that direct computer users to porn, gambling or other websites, Assistant U.S. Attorney James Aquilina said in a phone interview.

He also earned profits selling bot nets to others to spread spam and launch Web attacks, Aquilina said. Ancheta typically sold access to up to 10,000 machines at a time.

Bot herders sometimes flood commercial websites with bogus requests, shutting down the site. To end the attack and re-open for business, the website owner must pay a fee.

Ancheta forfeited $58,000 he had in cash and a 1993 BMW; he must also pay $19,000 in restitution to the federal government. He could also serve jail time. Sentencing is scheduled for May 1.

"This (hacking) community thinks it's immune to prosecution, but this case sends a message they are not," says Aquilina.

Ancheta's attorney, public defender Greg Wesley, had no comment.