December 28, 2005
U.S. Department of Justice
CRM
(202) 514-2007
TDD (202) 514-1888

## Man Pleads Guilty to Infecting Thousands of Computers Using Worm Program then Launching them in Denial of Service Attacks

## "Botnet" Investigation Led by U.S. Secret Service's Electronic Crimes Task Force and the Computer Hacking and Intellectual Property Unit of the U.S. Attorney's Office

SAN JOSE - United States Attorney Kevin V. Ryan announced that Anthony Scott Clark, 21, of Beaverton, Oregon, pleaded guilty yesterday afternoon in federal court in San Jose to launching a computer attack against the Internet auction site eBay in July and August 2003 with an army of infected computers he had amassed by using a computer worm program.

Mr. Clark pleaded guilty to a criminal information charging him with intentionally causing damage to a protected computer in violation of 18 U.S.C. §1030(a)(5)(A)(i), (a)(5)(B)(i), (c)(4)(A) and 2. The maximum statutory penalty for this offense is ten years imprisonment, a $250,000 fine or twice the gross gain or loss, and three years supervised release. However, any sentence following conviction would be imposed by the Court after consideration of the U.S. Sentencing Guidelines and the federal statute governing the imposition of a sentence, 18 U.S.C. § 3553. United States District Judge James Ware has scheduled a status hearing regarding sentencing for April 3, 2006, at 1:30 p.m.

In pleading guilty, Mr. Clark admitted as follows:

From July through August 2003, Mr. Clark participated with several others in distributed denial of service ("DDOS") attacks on the Internet against eBay, Inc. and other entities. A DDOS attack is one in which many compromised computers (or "bots) attack a single target, thereby causing a denial of service for legitimate users of the targeted system.

Mr. Clark and his accomplices accumulated approximately 20,000 "bots" by using a worm program that took advantage of a computer vulnerability in the Windows Operating System - the "Remote Procedure Call for Distributed Component Object Model," or RPC-DCOM vulnerability. The "bots" were then directed to a password-protected Internet Relay Chat (IRC) server, where they connected, logged in, and waited for instructions. When instructed to do so by Mr. Clark and his accomplices, the "bots" launched DDOS attacks at computers or computer networks connected to the Internet. Mr. Clark personally commanded the "bots" to launch DDOS attacks on the nameserver for eBay.com. As a result of these commands, Mr. Clark intentionally impaired the infected computers and eBay.com.

The prosecution is the result of an investigation by agents of the U.S. Secret Service's Electronic Crimes Task Force, which was overseen by the U.S. Attorney's Office's Computer Hacking and

Intellectual Property (CHIP) Unit. Christopher P. Sonderby, Chief of the CHIP Unit, is the Assistant U.S. Attorney prosecuting the case.

Further Information:

A copy of this press release and related court filings may be found on the U.S. Attorney's Office's website at www.usdoj.gov/usao/can.

Further procedural and docket information along with electronic court filings for criminal cases filed since February 2005 are available at https://ecf.cand.uscourts.gov/ (click on the link for "to retrieve documents from the court.")

Judges' calendars with schedules for upcoming court hearings can be viewed on the court's website at www.cand.uscourts.gov.

All press inquiries to the U.S. Attorney's Office should be directed to AUSA Christopher P. Sonderby at (408) 535-5037 or christopher.sonderby@usdoj.gov, or Luke Macaulay at (415) 436-6757 or Luke.Macaulay@usdoj.gov

ble doubt.

###