The Case of the “Zombie King”

Hacker Sentenced for Hijacking Computers for Profit

05/08/06

Imagine your computer being taken over by an outside force and used to send spam, to engage in cyber extortion, and to launch web attacks—all without you ever knowing about it.

Welcome to the not-so-brave new world of “zombies ”—Internet computers infected with malicious codes known as “bots” (short for “robots”) that secretly connect these PCs to websites or chat rooms where they can be controlled remotely.

It’s a growing problem. Some experts, for example, believe that networks of zombies—also called “botnets”—now send up to three-quarters of all spam. The collective force of botnets is also being used to launch major distributed denial-of-service attacks, knocking websites offline by overwhelming them with visits.

We’re fighting back…using the talents of our cyber professionals. One recent example: the investigation of the so-called “Zombie King”—Jeanson James Ancheta, a high-ranking member of a network of hackers called the “Botmaster Underground.”

Ancheta’s scheme had several dimensions, all designed to illegally line his pockets:

- Beginning in June 2004, Ancheta secretly hijacked tens of thousands of computers nationwide—including those at two military sites.
- Ancheta then set up a website to “rent” his army of infected computers, complete with guidelines on how many zombies would be needed to crash corporate webs of various sizes. The going rate? A minimum of 10,000 zombies at four cents a piece. He ended up renting or selling bots to at least 10 clients.
- In August 2004, Ancheta began working with a Florida teen, code-named “SoBe,” to grow his botnet army to more than 400,000 computers. He then signed up as an affiliate for online advertising agencies so he profited every time the owners of the bots were forced to download adware (software that displays ads and collects information about the websites you visit) and view the ads on their computers. In all, he pocketed about $60,000 in less than six months.

So how’d we catch him? We saw Ancheta’s web price list and opened an investigation. Our Los Angeles agents posed undercover in online chat rooms, asking Ancheta for help in launching cyber attacks. After bragging to us about making $1,000 in just two weeks, Ancheta sold us 2,000 bots, promising they’d be “enough to drop a site.” We seized Ancheta’s computer in December 2004 and eventually put him out of business for good in May 2005 when we disabled the servers he was using. After gathering more evidence, we arrested Ancheta in November 2005. On Monday, Ancheta—who in January became the first person to plead guilty to federal charges of hijacking computers for profit—was sentenced to 57 months in prison, plus three years of supervised release. Additionally, he was ordered to make restitution for the damage he caused the two military sites.

How can you keep your computer from being turned into a “zombie”? At the very least, use a computer firewall, keep your anti-virus software up to date, and install the latest security patches for your operating system. And be suspicious if your Internet connection unexpectedly slows to a virtual halt and refuses to perform even the simplest functions—possible warning signs that your computer has been hijacked.

Resources: FBI Cyber Program

Story Index

By Date

By Subject
- Art Theft
- Civil Rights
- Counterterrorism
- Crimes Against Children
- Criminal Justice Information Services
- Cyber Crimes
- Director/FBI Leadership
- Field Cases
- Foreign Counterintelligence
- General
- History
- Intelligence
- International
- Lab/Operational Technology
- Linguist/Translation Program
- Major Thefts/Violent Crime
- Organized Crime/Drugs
- Partnerships
- Public/Community Outreach
- Public Corruption
- Recruiting/Diversity
- Responding to Your Concerns
- Technology
- Training
- White-Collar Crime