Operation: Bot Roast

'Bot-herders' Charged as Part of Initiative

06/13//07

They're called "bot-herders:" hackers who install malicious software on computers through the Internet without the owners' knowledge. Once the software is loaded, they can control the computer remotely. And once they've compromised enough computers, they have a robot network or botnet.

Some botnets are huge: tens of thousands of infected computers. Or more. As a result of Operation Bot Roast, an ongoing and coordinated initiative to disrupt and dismantle these bot-herders, we've identified about 1 million computers across the country that have been compromised.

More Information

- Press Release
- Protect Your Computer

The FBI has also charged numerous individuals with cyber crimes around the nation as a direct result of the coordinated operation, including:

- Robert Alan Soloway of Seattle, Washington, is accused of using botnets to send tens of millions of spam messages touting his website;
- James C. Brewer of Arlington, Texas, is accused of infecting tens of thousands of computers worldwide, including some at Chicago-area hospitals; and
- Jason Michael Downey of Covington, Kentucky, is charged with using botnets to disable other systems.

As the investigations continue to unfold, it is possible we will uncover more victims. Here are some important things to remember:

- First, if you believe your computer has been compromised, **do not call the FBI directly**. We are not in a position to provide technical assistance. Please see Ways to Protect Your Computer.
- Second, if you determine you are a victim, then we encourage you to file a complaint online through our Internet Crime Complaint Center.
- Third, **the FBI will not contact you online and request your personal information** : Be wary of fraud schemes that request this type of information, especially via unsolicited e-mails.

Resources

- Botnet Consumer Alert
- Botnet Tips
- FBI Internet Crime Complaint Center

Operation Bot Roast was launched because the national security implications of the growing botnet threat are broad. The hackers may use the computers themselves, or they may rent out their botnets to the highest bidder. The more computers they control, the more they can charge their clients.

A bot-herder can do a lot with compromised computers:

- Steal the computer owner's identity;
- Launch massive spam campaigns;
- Engage in click-fraud—schemes which artificially inflate the number of visitors to a website; and
- Launch denial of service attacks that can cripple web servers and crash sites.

One of the difficulties in fighting this type of cyber crime is that it is difficult for computer owners to know if their machines have been infected. There is no easy way to tell, unfortunately. It may be running slowly, your outbox may be full of mail you didn't send, and you may get mail stating you've sent spam.

"The majority of the victims are not even aware that their computers have been compromised or their personal information exploited," said FBI Assistant Director James Finch, who heads our Cyber Division.

That's why we urge every computer owner to implement the security precautions that are available. Prevention is always better than reaction.

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