

An Epic Opportunity for Your Business.



www.internetnews.com/bus-news/article.php/3683686

[Back to Article](#)

Four Bot Herders Get Put Out To Pasture

By [Andy Patrizio](#)

June 15, 2007

Your spam filters have ever so slightly less work to do today, thanks to several arrests of bot herders by the FBI.

A bot herder is someone who controls thousands if not tens of thousands of compromised computers with hidden software to fire off spam e-mails. These compromised computers are called "bots," or sometimes "zombies," since they operate mindlessly.

Bot herders have control of these computers and sell their use to spammers, who send out junk mail for pump-and-dump stock scams, mortgages and male sexual performance drugs. The bot herder sends the spam letter to all of his compromised computers, along with a list of e-mail targets, and the bots then pump the letters out.



As part of an effort cleverly titled Operation Bot Roast, the FBI recently made three big arrests. James C. Brewer of Arlington, Texas, is alleged to have operated a botnet that infected Chicago area hospitals and tens of thousands of computers worldwide.

Jason Michael Downey of Covington, Kentucky, is charged with a distributed denial of service attack (DDOS) while Robert Alan Soloway of Seattle, Washington, is also alleged to have operated a large botnet network.

Separately, Adam Vitale of Brooklyn, N.Y. pled guilty this week in federal court to breaking anti-spam laws by flooding AOL users with spam. He and a partner claimed to be making \$40,000 a month. Both men will be sentenced on September 13 and face up to 11 years in jail.

No one knows how many bot herders are out there. Matthew Sweet, CEO of Unspam Technologies, said there are just under 18,000 harvesters on the Internet, which crawl the network looking for e-mail addresses, so he doubts the herder population is larger than that.

Four arrests, therefore, isn't huge, but it's a start.

"This is not going to solve the problem in one fell swoop but it changes the economy of sending spam," Sweet told *internetnews.com*. "If you're an 18-year-old kid and think spam is a great way to make some money, seeing a guy go to jail for 10 years could have an affect on you."

Other security firms are happy to see the FBI is taking this issue seriously.

"The FBI's actions in raising the public's level of security awareness regarding botnets and moving against this type of activity are to be applauded," said Yuval Ben-Itzhak, CTO of security vendor Finjan, in a statement.

And Paul Henry, vice president of technology evangelism for Secure Computing, told *internetnews.com* "I applaud their effort to apply more cycles at getting cybercriminals. They've taken out three bot herders who controlled more than one million PCs."

While four arrests are hardly cracking the community of bot herders, the security experts see good news in one aspect: they are getting bad guys in the U.S. It would be a lot harder to get them in Russia.

"This shows spammers don't have law enforcement kryptonite. A substantial percentage are operating within the U.S. and all are leaving a track that with some resources and tenacity can be found," said Sweet.

Mike Irwin, COO for spyware software detection company Webroot, added "There's a lot of independent contractors

out there, but probably the bigger challenge here is, if you notice the folks identified were all within the U.S. That helps because they are all within one federal jurisdiction. It gets a lot more challenging when it starts to cross borders."

Henry said the U.S. has formed treaties with friendly nations to deal with cross-border jurisdiction, but many of the worst offenders are in countries that have chilly relations with the U.S., like China and Russia. Still, law enforcement is finally coming around to dealing with the problem.

"Part of the issue is that since 9/11, it's been a resource issue for most law enforcement," said Henry. "They have not had the necessary resources to really apply their time to cybercrime. They had to concentrate on homeland defense. Now that they have those systems in place, we're seeing more time devoted to cybercrime and white collar crime."

Sweet noted that in most cases, there's some sort of public/private partnership between the FBI and software firms. He, Henry and Irwin more or less confirmed this by declining to comment on their firms' work with law enforcement.

[Contact internetnews.com staff](#)

Jupiter Online Media:



Search:

[Jupitermedia Corporation](#) has two divisions: [Jupiterimages](#) and [Jupiter Online Media](#)

[Jupitermedia Corporate Info](#)

Copyright 2007 Jupitermedia Corporation All Rights Reserved.
[Legal Notices](#), [Licensing](#), [Reprints](#), & [Permissions](#), [Privacy Policy](#).

[Web Hosting](#) | [Newsletters](#) | [Tech Jobs](#) | [Shopping](#) | [E-mail Offers](#)