



- Capital
- Industries
- Profiles
- > Q&A
- Executives
- Entrepreneurs
- Venture Capitalists
- Policy Makers & Pundits
- Regions
- Briefings
- Metrics

- Research
- Newsletters
- Events

Get 4 FREE Issues! **RED HERRING** 50 BIG DEALS

▶ **Subscribe Now**

▶ **Customer Service**

Advertisement

- MARKETS -

NYSE	8112.74	+6.19
NSDQ	2309.39	+3.57
S&P	1282.38	+2.30
Delayed 20 mins.		



Q&A

Email this article Printable format Letter to

Q&A: Bot-Buster Merrick Furst

*The associate dean at Georgia Tech's College of Computing says botnets are security threat.*

January 27, 2006

The Internet worm Zotob that crashed computer networks at major companies including *The New York Times* and credit card company Visa brought into focus the danger of bots. Short for robots, bots are computers that have been infected by worms, viruses, or spyware so they can be controlled externally by a hacker (see [Zotob Costs \\$97K per Company](#) and [Top Security Trends for 2006](#)).

Botnets or bot armies are large networks of thousands of machines under the control of an attacker who could potentially use the computers for criminal activities including stealing financial information and proprietary data stored on a computer.

Because of the potential of bots to do great harm, law enforcement has gone on high alert. Their efforts appear to be paying off. On Monday, Jeanson James Ancheta, a 20-year-old in Downey, California, pleaded guilty to hijacking thousands of com hacker launched destructive attacks and sent huge quantities of spam across the Internet.

Mr. Ancheta made about \$60,000 in advertising affiliate proceeds through the surreptitious installation of adware on about 400,000 compromised computers, said the assistant U.S. attorney's office at the Department of Justice in California.

One of the biggest bot-busters is Dr. Merrick Furst, distinguished professor and associate dean at the College of Computing at Georgia Tech. Dr. Furst has been tracking botnets for the last two years, researching how they are created, how they speak to each other, and how big the problem is.

During October, the College of



Dr. Merrick Furst  
Credit: College of Computing, Georgia Technology.

- ADVERTISEMENT -

Computing spun off a startup called Damballa, named after the most-important god of the voodoo religion.

Dr. Furst, who is also the president of Damballa, worked with the FBI on the Zotob case and helped federal investigators track botnets. In an interview with *Red Herring*, he said botnets are being generated at an astounding rate and traditional methods to fight them are proving ineffective. Below are edited excerpts of the conversation:

**Q: How big do you think is the problem of botnets?**

**A:** More than a quarter-million new machines are conscripted every day by bots. We are currently tracking 10 million machines that we think are infected. And these are spread all over the world though we find a large number to be in Asia. There are lots of Asia running pirated software, so they're not getting the latest security patches and these can become bots.

In the U.S., 25 percent of bots that we see are AOL machines and 10 percent are MSN machines spread through worms and viruses that carry them. During a typical seven-day period we're tracking over six bot armies that were forming and each of these armies had thousands of

We found 700,000 computers infected during the last few months. In a typical month, there are 6,000 command-and-control points up and running. It is how a botnet master talks to the machines like an HQ [headquarters] for the botmaster.

**Q: What are these botnets being used for?**

**A:** Bot armies have become platforms for carrying out criminal fraud. One bot that is acting as a keylogger can pick up all the keystrokes that you type and it will send a snapshot of the screen to the botmaster. The botmaster can see a slideshow of what you are doing on your computer terminal. More than 80 percent of the data is being sent by bot armies since they are hard to pick up by spam filters.

Bots are being used for denial of service attacks. A botmaster will have 100,000 machines and can use them to launch these attacks. They even use bot armies to commit click fraud. A lot of email comes from bot armies. There's been a big transformation over the last year and a half in learning how to make money using the botnets and it makes it very dangerous.

**Q: How effective are the traditional approaches to combating the problem?**

**A:** They are obviously not that effective since we think there may be 75 million machines worldwide. Normally, people try to protect individual machines. They have standard, traditional methods for protection, which is signature-based protection or behavior-based methods.

The problem is that botmasters defeat those. They keep building new software so signature-based protection doesn't work and they have more machines available. So they can divide their machines into smaller groups and keep their messages under the threshold that will be flagged by behavior-based network protection.

**Q: How does your startup, Damballa, tackle the botnets issue?**

**A:** We have taken a nonconventional approach. We studied how these bot armies communicate with each other and the patterns they have. We have been monitoring networks so we can pick



formation of these armies. Imagine if you could listen in on all the interactions that computers are having and recognize that some of those are about forming a bot army.

Our customer right now is the government, which is worried because these bots can be directed against infrastructure. They can be used to take out cellular networks through distributed denial of service attacks and used to direct anonymous threats.

#### RELATED ARTICLES

### **Banks Press for Data Safety**

Financial institutions want computer service providers to do more in guarding against security breaches.

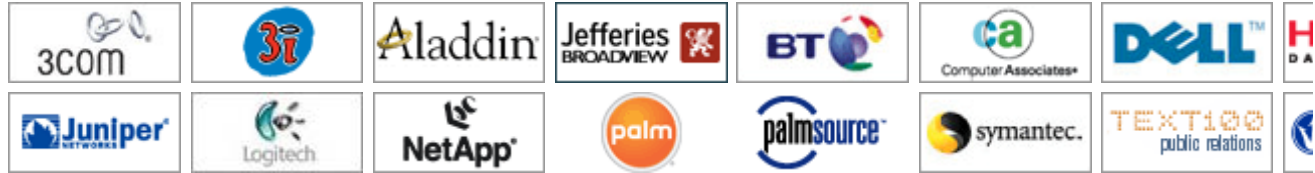
### **Gates Funds Community Tech**

Microsoft head bankrolls local technology centers worldwide with \$25.2 million.

#### RECENT ARTICLES >>

- [Q&A: Craig Conway](#)
- [Q&A: Paul Twomey](#)
- [Q&A: SonoSite's Kevin Goodwin](#)
- [Q&A: GTC's Geoffrey Cox](#)
- [Q&A: Larry Ellingson](#)
- [Q&A: Frans van Houten](#)

#### RED HERRING Sponsors



[Articles](#) | [Blog](#) | [Research](#) | [Newsletters](#) | [Events](#)

[New User Registration](#) | [Search](#) | [About Us](#) | [Letter from the Editor](#) | [Advertising Info](#) | [Magazine Customer Service](#) | [Contact Us](#) | [Careers](#) | [RS](#)

© 1993-2006 Red Herring, Inc. All rights reserved.