

SEARCH

THE WEB

CNN.com

SEARCH

Powered by YAHOO! search

Home Page

World

U.S.

Weather

Business

Sports

Politics

Law

Technology

Science & Space

Health

Entertainment

Travel

Education

Special Reports

Video

Autos

Predict the movie winners and you could win A HOME THEATER SYSTEM

PLAY NOW

SERVICES

CNN Pipeline

E-mail Newsletters

Your E-mail Alerts

Podcasts POD

RSS XML

CNNtoGO

Contact Us

SEARCH

WEB CNN.com

SEARCH

SEARCH Powered by

YAHOO! search

TECHNOLOGY

CNNACCESS

ARCHIVE >>

Expert: Botnets No. 1 emerging Internet threat

Tuesday, January 31, 2006; Posted: 2:59 p.m. EST (19:59 GMT)

ATLANTA, Georgia (CNN) -- A "botnet" is a network of zombie computers -- thousands surreptitiously are infected with code that allows an unauthorized user to control them via the Internet. The computers can be used to spread spam, launch denial-of-service attacks against Web sites and conduct fraudulent activities.

Merrick Furst, professor of computing and associate dean for undergraduate programs at Georgia Tech's College of Computing, is conducting extensive research into botnets. He talked recently with CNN technology correspondent Daniel Sieberg.

SIEBERG: How do we understand what a botnet is exactly?

FURST: A botmaster is a criminal who wants to use your computer as a resource in some way. So he or she buys software and has that software released onto the Internet in a way that's self-propagating either as a virus or worms. It then finds its way on to your computer without you knowing about it. At which point, the botmaster has control of your computer. They can use your computer to commit fraud.

SIEBERG: And so he could have how many computers under his control at any one time?

FURST: We've watched bot armies grow at a bizarre rate, 350,000 machines. Typical bot army sizes range between 10,000 machines and 100,000 machines.

SIEBERG: What can they do using all



Merrick Furst, associate dean for undergraduate programs at Georgia Tech's College of Computing

advertiser links [what's this?](#)


2.75% Fixed Student Loan Consolidation
70% lower monthly student loan payment at NextStudent. Consolidation rate locked...
www.nextstudent.com

H&R Block - Official Site
Fast, easy, accurate tax prep - online, software, or in our office.
www.hrblock.com

Mortgage and Refinance Quotes
Apply today to get up to 4 quotes from top lenders. Any credit OK. Refinance,...
www.lowratesource.com

Technology Essentials

- [Camcorders](#)
- [Computer Technology](#)
- [Tech Support](#)



WATCH

Browse/Search

Don't let computer zombies spook your computer (4:30)



Search Jobs MORE OPTIONS

Enter Keywords

Enter City ALL

careerbuilder.com SEARCH

GET IT NOW >

See where

CNN Pipeline

can take you.

GET IT NOW >

these computers?

FURST: The botmasters could do a lot of things with their bot armies to be able to make money. They can do something like a denial-of-service attack. ... If a botmaster has, let's say 100,000 machines in their control, then they control huge amounts of bandwidth. So they can, for example, attack a company and not let anyone else get to that company's Web site.

SIEBERG: Really shutting the Web site down in a sense.

FURST: Shutting it down is called denial of service. Often what will happen is that the botmaster will contact the site beforehand and say, "We will do this on Friday unless you pay us on Thursday."

SIEBERG: That's extortion.

FURST: It's straight extortion. There's a lot of that going on.

SIEBERG: And they can also steal people's information?

FURST: Key loggers can be used to get credit card information, bank account information. There are many reports now that people are having their online banking account emptied, their brokerage account emptied, by people who get this information.

SIEBERG: There's another thing that's a little bit complicated for some people -- click fraud.

FURST: People are worried that click fraud might be a threat to some of the business models on the Internet, for example, the business model that Google has where every time you click on an ad, Google gets paid by an advertiser.

So let me tell you how a botmaster makes money with click fraud. ... They'll build a Web site that looks like a normal Web site. They'll put up banner ads, or other types of ads on their Web site, and these are ads served up by Google. Google contracts an advertiser to put up ads on sites -- [unwittingly] contracts the botmaster online to put up ads on that botmaster's site. ... So [the botmaster] commands the machines in his bot army to click on the ads on this site. Every time one of his machines click, the message goes back to Google, Google charges the advertiser, the advertiser pays Google, Google keeps 20 percent and [unwittingly] gives 80 percent to the botmaster. ... Let's say even if [the botmaster] controls a small army of 5,000 machines, which is very small in this game -- he can make \$15,000 a month in click fraud.

SIEBERG: And spam?

FURST: Over 80 percent of all spam messages are coming from bot armies right now. A botmaster will have 100,000 machines under his control. He'll contract to send a million [e-mail] messages, and he'll have each machine send out only 10 messages. ... It's very hard for you as the owner of a machine that is compromised to know that 10 [e-mail] messages went out on any given day.

SIEBERG: That goes back to how someone will know that their computer is part of this bot army.

FURST: Yeah, it's virtually impossible for an average person to know whether or not their machine is conscripted into a bot army. The botmasters are financially motivated; they have great programmers that they're working with.

A lot of times these bots will get picked up, but they get picked up days or weeks after

YOUR E-MAIL ALERTS

Computer Security

Internet

CNN Access

Daniel Sieberg

or [Create Your Own](#)

[Manage Alerts](#) | [What Is This?](#)

they've been actually on your machines. So even if you run something like Norton Antivirus, or Symantec or McAfee, ISS, one of those services, it's still the case that you're very susceptible. And most people don't even run these services.

SIEBERG: Is there any way to know how many computers out there have a botnet program on their system?

FURST: We're pretty sure it's at least 7 percent of the Internet. Typical numbers range from around 75 million to 100 million machines that are currently conscripted. In our labs, in our resources, we know the IP addresses of 12 million machines that are currently part of bot armies.

SIEBERG: Wow. And how much has it grown in the last couple of years?

FURST: Well, it was 10 million when I looked at it about three weeks ago. So it's growing very fast. A couple of hundred thousand machines are going to get conscripted every month -- that's what the estimates are.

SIEBERG: OK.

FURST: Now we've actually had some success out of the College of Computing at Georgia Tech. In the summer of [last] year, two of our researchers were contacted by the FBI. ... The FBI was wondering whether or not our group had any knowledge about this outbreak of a large worm called Mytob/Zotob. And it turns out that bot army happened to be a bot army that the [researchers] were tracking, and they actually tracked it from inception. ... And they found the IP address of a man who's now ... sitting in a jail in Turkey, and criminal prosecution is in progress. But it's very rare -- getting that type of actual information is very rare.

SIEBERG: Now, about trust fraud, another way of getting money for these guys.

FURST: Yes, the trust fraud is actually very scary, and it goes right at business models of sites like eBay. We've intercepted software that does the following. ... It creates a Web site that looks like a normal EBay seller site, for example, a site that sells cameras.

So then the botmaster gets his army to send 15,000 zombies to come to this site and buy things with stolen credit cards, and with each transaction, it boosts the seller's ratings so then eventually the seller's rating becomes platinum. At which point there's a fraudulent seller that you and I would go to and think, "Oh, this site is a great site to buy cameras; there are 15,000 happy customers." So we spend our money with our legitimate credit cards, and now we're out of money.


Story Tools

[SAVE THIS](#)
[E-MAILTHIS](#)

[PRINT THIS](#)
[MOST POPULAR](#)

advertisement

[Click Here to try 4 Free Trial Issues of Time!](#)



SCI-TECH

Section Page | Video | Business 2.0 


CNN/Money: [Shrugging off Google's miss](#)

- [New worm relies on old trick](#)
- [Tech firms decline human rights briefing](#)
- [Members of secretive group indicted in piracy plot](#)

TOP STORIES


Home Page | Video | Most Popular

[Postal shooter's former neighbor found dead](#)



- [Bush: 'We can't be isolationists'](#)
- [Andrea Yates leaving jail, going to mental hospital](#)
- [Shirt tales different for Sheehan, Republican's wife](#)

[International Edition](#)

Languages 

[CNN TV](#)

[CNN International](#)

[Headline News](#)

[Transcripts](#)

[Advertise with Us](#)

[About Us](#)

SEARCH


THE WEB


CNN.com

SEARCH

Powered by 

© 2006 Cable News Network LP, LLLP.
A Time Warner Company. All Rights Reserved.
[Terms](#) under which this service is provided to you.
Read our [privacy guidelines](#). [Contact us](#).

 External sites open in new window; not endorsed by CNN.com

 Pay service with live and archived video. [Learn more](#)

 [Download audio news](#) |  [Add RSS headlines](#)