Security
April 21, 2009 9:00 PM PDT

Finjan finds botnet of 1.9 million infected computers

by Elinor Mills

SAN FRANCISCO--Security firm Finjan has uncovered what it says is one of the largest bot networks controlled by a single cybergang, with 1.9 million infected zombie computers.

The botnet has been in use since February, is hosted in the Ukraine, and is controlled by a gang of six people who are instructing the Windows XP-based machines to copy files, record keystrokes, send spam, and take screenshots, Ophir Shalitin, Finjan marketing director, said in an interview on the eve of the RSA security conference.

The gang has compromised computers in 77 government-owned domains in the U.S. and elsewhere, he said. Nearly half of the infected computers were in the United States. Nearly 80 percent of the infected computers are running Internet Explorer, while 15 percent are using **Firefox**, **Finjan** said.

The criminals operating the botnet can make as much as $190,000 in one day renting out the zombies to others, according to Finjan Chief Technology Officer Yuval Ben-Itzhak.

The command-and-control server being used to control the infected PCs is instructing the bots to download and execute a Trojan horse, which is detected by only 4 out of 39 antivirus products, said Shalitin.

The Trojan installs malicious executables that communicate with other computers, inject code into processes, visit Web sites, and other activities the user has no involvement with, according to **a post on the Finjan Malicious Code Research**

Center blog.

"Overall, the cybergang can remotely execute anything it likes on the infected computers," the post says.

Elinor Mills covers Internet security and privacy. She joined CNET News in 2005 after working as a foreign correspondent for Reuters in Portugal and writing for The Industry Standard, the IDG News Service, and the Associated Press. E-mail Elinor.

Topics: **News**, **Vulnerabilities & attacks**

Tags: **Finjan**, **botnet**, **Ukraine**, **RSA 2009**

Share: Digg Del.icio.us Reddit Yahoo! Buzz

Related

From CNET

Gates: Cyberattacks a constant threat

I'm officially dropping out of the Twitter gab fest

Conficker wakes up, updates via P2P and drops payload

From around the web

Gadgetwise: Mac Security III: The Rise o... The New York Times

Conficker Removal Reminders Washington Post Blogs - Faster...

More related posts powered by Sphere