Security
April 22, 2009 5:09 PM PDT

Botnet expert suggests hitting cybercriminals in pocket book

by Elinor Mills

SAN FRANCISCO--Technology is not enough to help the security industry keep botnets from stealing peoples' money and committing denial-of-service attacks, a top botnet researcher said on Wednesday. His suggestion? Stop the flow of money to their coffers.

"We need to disrupt their business model and make it hard for them to carry out their attacks and make money," Joe Stewart, a security researcher at **SecureWorks**, said in an interview at the **RSA 2009** security conference here.

"Right now, it's risky to surf the Internet with a PC," he said. "I would like to see us return to a time when you could surf the Internet and trust that your computer wasn't going to get infected."

Computers can be infected in any number of ways, but typically they get a Trojan or other malicious program downloaded onto them without the owner's knowledge, which happens either from visiting a Web site with malicious code on it or opening malicious attachments in e-mail.

Once infected, depending on the attack, a computer can be controlled by remote attackers who are able to steal data or instruct the computer and other so-called zombies into sending spam or launching distributed denial-of-service attacks to shut down Web sites.

Researchers have focused on trying to stop attacks, but once they get a botnet operator kicked offline by shutting down its hosting provider it's usually not long before the

botnet cranks back up with its command-and-control server at a different location, he said. For example, four months after a major botnet hoster, McColo, was shut down in November, the spam volumes **were back up to normal levels**.

Specifically, victims should be encouraged to seek reimbursement when they are charged for things like purchasing software that masquerades as a legitimate antivirus program, said Stewart, who created an ingenious **eye-chart program** that PC users can use to test whether their computers are infected with Conficker. The eye chart was needed because Conficker blocks access to security sites people would normally visit to check for infection.

The industry should also create teams of researchers that would focus on a single crime group or operation much like police stay on the trail of a particular real-world organized crime gang until everyone is arrested, Stewart said.

The organization would need funding, which could possibly come from the companies that seem to be impacted the most from cybercrime, like credit card processors, he said.

Law enforcement efforts are thwarted because officials in other countries where cybergangs are based often can't be convinced to cooperate, he said. Getting countries to sign a global anti-Internet abuse accord would be ideal, he said.

Meanwhile, national CERT (Computer Emergency Readiness Team) organizations should be given authority to fight botnets, by ordering Internet service providers to shut down hosting providers, Stewart said. In South Korea, for example, malicious Internet activity dropped drastically when the CERT three got teeth, he added.

Stewart is scheduled to give a presentation on his idea during a session Thursday at RSA and at an upcoming Interpol meeting.

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: **Vulnerabilities & attacks**

Tags: **RSA 2009**, **SecureWorks**, **Joe Stewart**, **botnets**

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

Related

From CNET

The Cold War moves to cyberspace

Finjan finds botnet of 1.9 million infected computers

Gates: Cyberattacks a constant threat

From around the web

Conficker Removal Reminders
Washington Post Blogs - Faster...

Another stage for American Idols--the iP... CNET News

More related posts powered by Sphere