



CREATE YOUR OWN WIRED COVER



GO

POWERED BY XEROX

Top Stories

Politics : Law 

Stiffer Cyber Laws to Crack Down on Botnets, Spyware

By Luke O'Brien  06.04.07 | 2:00 AM



The I-SPY Act introduced by Rep. Zoe Lofgren (D-California) would impose five-year sentences and/or fines for use of software such as botnets to commit federal offenses.

Photo: AP / Haraz Ghanbari

WASHINGTON -- Federal lawmakers confronting a plague of botnet infections, denial-of-service extortion schemes and spyware are going on the counter-offensive with two new bills that would make it easier for federal prosecutors to charge cybercriminals, while bringing computer intrusion under the ambit of the mob-busting RICO Act.

Together, the Cyber-Security Enhancement Act and the Internet Spyware (I-SPY) Prevention Act would represent one of the more significant updates to federal computer-crime law in the last two decades.

Around 30 percent of malicious internet activity took place or originated in the United States in the second half of last year, according to information from Symantec. China was second at 10 percent. Prominent among today's threats are bots -- a type of malicious software that secretly puts a vulnerable PC under the control of an attacker, who can direct thousands of computers at once. Organized cybercriminals routinely use networks of bots to launder spam, steal passwords for online banking and launch denial-of-service attacks like those that recently plagued the small European nation of Estonia after it angered Russian nationalists.

"You're looking at a new species of criminal conduct," says Roma Theus, a white-collar crime expert at the Defense Research Institute and a former federal prosecutor. "We have to look beyond where we are today and think about where we might be ten years from today."

The Cyber-Security Enhancement Act, introduced by Rep. Adam Schiff (D-California), would do just that, stiffening penalties and sentencing times for cybercriminals by classifying computer-fraud offenses as a predicate offense for the Racketeer Influenced and Corrupt Organizations, or RICO, law. Authorities could also seize any ill-gotten gains a crook may have obtained through online rackets.

The measure also adjusts the damage threshold that qualifies a cybercrime receive FBI attention. Currently, a financial loss of \$5,000 spread out among victims makes an intrusion into a federal case; under the bill, damaging 10 or more computers in a year would automatically qualify, even with no financial harm.

This bill has cheered many advocates for tougher laws on cybercrime. "In our discussions with law enforcement, that \$5,000 limit is a major sticking point in terms of not being able to go after these criminals," says Rob Tai, the manager of cybercrime prevention for the Business Software Alliance, which represents the commercial software industry and supports both bills.

The I-SPY Act, introduced by Rep. Zoe Lofgren (D-California), amends the same federal computer crimes statute by setting a five-year sentence and/or fines for anyone caught using subversive software "in furtherance" of a federal criminal offense. Scam artists who distribute software coded with keystroke loggers or other covert functions, and who use it to steal Social Security numbers, credit card numbers, passwords or any personal identification information could face new charges. So could hoods using spyware to "impair" a computer's security system while trying to defraud another person, although the prison time for that offense drops to two years.

The bill is a nice step forward but only part of a much-needed collection of tools to combat spyware violations, according to David Sohn, senior policy counsel at the Center for Democracy and Technology. "It's adding an additional enforcement arrow to the quiver," Sohn said.

Both measures modify the Computer Fraud and Abuse Act, the federal anti-hacking bill enacted in 1986. Originally intended to protect only federal government computers and financial institutions, the CFAA has been amended several times since then, most recently in 2001, when the Patriot Act raised the maximum penalties, among other tweaks.

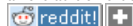
Not everyone thinks the latest crop of bills is the correct response to shifting cyberthreats. "I'm not sure it's completely necessary," says Andy Serwin, a noted cyberspace lawyer and the author of a book on information security and privacy laws. "How much burden do you put on business?"

The Federal Trade Commission already enforces cyberfraud, and state and federal laws cover more than enough ground to allow for prosecution, Serwin argues. Increased legislation might wind up criminalizing legitimate software, such as Microsoft's updater, which automatically installs programs on computers and might technically be spyware under the new legislation, he says.

Besides, Serwin adds, "The guy who's going to do the really malicious stuff is going to do it anyway. And he may do it offshore, so there's no way to get at him."

Theus disagrees. He says that the government could extradite wrongdoers, or even seize them, ala Manuel Noriega. "If someone is under the misapprehension that they can be outside the U.S. and commit a crime that has effects inside the U.S. (and avoid sanctions), that person is going to be terribly surprised."

So far such extraditions are virtually unheard of. In the U.K., Gary McKinnon, a 41-year-old man accused of penetrating over 90 unclassified U.S. military computers in 2001 and 2002, has delayed extradition for years, even while admitting to the hacking spree. In April he lost a court challenge to an extradition order, and is now on a final appeal to the U.K. Parliament's Law Lords.



Add this to:
[Digg](#)
[Del.icio.us](#)
[Sphere](#)

See Also:

- [Desperate Botnet Battlers Call for an Internet Driver's License](#)
- [Wired Blog: Threat Level](#)
- [I'm the Blue Security Spammer](#)
- [Hackers Admit to Wave of Attacks](#)
- [A Chinese Call to Hack U.S.](#)
- [Hacker War Rages in Holy Land](#)
- [Both Sides Hacked Over Kashmir](#)
- [Search Wired](#)

Top Stories

-  Email Article
-  Print
-  Full Page
-  Comments

Sponsored by:



UPDATE IN PROGRESS

We are currently performing maintenance tasks to improve the site, and the Please try again shortly.