

Defeating Today's Cyber Criminals

The Changing Realities of Cyber Crime

- Money Fuels Today's Cyber Crime
Cyber criminals used to write malicious code for bragging rights. Not anymore. Cyber crime today is about money. For example, cyber criminals steal social security or credit card numbers, then often sell that data online at a significant profit to others who will commit identity theft.
- Cyber Criminals Are Technologically Sophisticated
To reap ever greater profits, cyber criminals invent or refine their techniques constantly. The best example is the rise of botnets. Botnets are vast, surreptitiously controlled networks of compromised computers that can be used to carry out a variety of illegal activities, including disseminating spam, phishing, and launching denial-of-service attacks.
- The Rise of Global Online Organized Crime
Cyber criminals are not isolated actors. They are part of a well-organized, massive, illicit underground economy. They form sophisticated supply chains that often span continents.
- America is The Number One Target
No country is spared by cyber criminals, but according to a recent Symantec report, the US is the target of 30% of all malicious cyber activity, which is three times more than the number two country, China.

What Congress Should Do

Resource constraints and gaps in federal criminal law hamper the prosecution of these new and emerging forms of cyber crime. HR 2290, The Cyber Security Enhancement Act (and closely related legislation in the Senate) would make five crucial improvements to U.S. law:

1. Target botnets. Current law requires that a suspect cause \$5,000 of damage to computers before he can be charged: to reach that threshold, prosecutors must track down many individuals whose computers were hijacked.
 - Congress should simply criminalize accessing a computer without authorization, to steal means of identification, or causing damage to ten or more computers.
2. Address new forms of cyber extortion. Under existing law, cyber extortion requires a threat to cause damage to a computer.
 - Congress should clarify that making a threat to access a computer unless the victim complies with demands for money or items of value, regardless of whether he threatens to damage the computer itself, is also cyber extortion.
3. Close the interstate communications loophole: today, a federal cyber crime must involve interstate communication, even though serious crimes like insider attacks may be committed within a state's borders.
 - Congress should expand federal jurisdiction to crimes targeting computers used in or affecting interstate commerce.
4. Attack organized crime, strengthen penalties: currently, federal law is not well-suited to cracking down on online organized crime and penalties are insufficiently deterrent.
 - Congress should add computer crimes to the list of racketeering offenses ("RICO predicates"), create an explicit charge of conspiracy to commit cyber crime, and stiffen cyber crime penalties through forfeiture and deterrent sentences.
5. Increase funding for law enforcement: while BSA gives high marks to law enforcement for their efforts, we believe their resources are seriously constrained even though they need to constantly upgrade the training and equipment of their agents.
 - Congress should authorize additional funding of \$10 million a year for the Department of Justice, FBI, and Secret Service.

For more information, contact Franck Journoud at franckj@bsa.org or (202) 530 5128.