Contact Us
- Your Local FBI Office
- Overseas Offices
- Submit a Crime Tip
- Report Internet Crime
- More Contacts

Learn About Us
- Quick Facts
- What We Investigate
- Natl. Security Branch
- Information Technology
- Fingerprints & Training
- Laboratory Services
- Reports & Publications
- History
- More About Us

Get Our News
- Press Room
- E-mail Updates
- News Feeds

Be Crime Smart
- Wanted by the FBI
- More Protections

Use Our Resources
- For Law Enforcement
- For Communities
- For Researchers
- More Services

Visit Our Kids' Page

Apply for a Job

Headline Archives

THE CYBER THREAT TODAY
Major Attacks on the Rise

10/17/08

Shawn Henry, Assistant Director of the FBI's Cyber Division.

Crooks and spies using the Internet to commit crimes against U.S. businesses and to attack government networks are getting more sophisticated, and the increasing number of such crimes not only impacts the economy but threatens national security.

That's the message Shawn Henry, recently appointed head of our Cyber Division, delivered to a group of reporters on Wednesday, revealing that we have thousands of open cases into cyber crimes and organized cyber attacks and detailing our strategy to protect the nation's networks.

One case in point: We joined our international partners yesterday in announcing a major takedown of a transnational criminal network that was buying and selling stolen financial information through an online forum known as "Dark Market."

"The business of the United States is done on the Internet," said Henry, a veteran cyber crime investigator. And the information that flows electronically 24/7 is increasingly the target of not only identity thieves and scammers, but organized crime groups, terrorists, and overseas governments.

"There are a number of countries who have an interest in stealing information from the United States," Henry said, explaining that as many as two dozen nations have taken an "aggressive interest" in penetrating our networks. In the past year, he added, "the malicious activity has become much more prevalent."

Malicious activity could come in the form of attacks that deny access to websites, that compromise sensitive information, or that introduce "botnets" that spread viruses and covertly co-opt computers to carry out data theft.

"There are a number of countries who have an interest in stealing information from the United States," Henry said, explaining that as many as two dozen nations have taken an "aggressive interest" in penetrating our networks.

New groups of hackers—virtual gangs—are a growing threat as well, banding together to pool their expertise and carry out coordinated cyber attacks. Henry pointed out that in years gone by, if a gang wanted to rob a bank, it needed crooks with various skills—safe cracker, get-away driver, look-out, etc. That's essentially what we're seeing in the cyber world today, only these virtual gang members have never met in the physical world. "There are organized groups that are very successful," Henry said.

The 3 Ps. To address the rising threat, the Cyber Division has a threefold strategic plan—"Prioritize, Proactive, Partnerships."

By prioritizing our efforts, we can go after the most critical threats. Being proactive means adopting the same time-tested investigative techniques that have been so successful in our physical crime investigations—the use of informants, electronic surveillance, and placement of undercover agents to penetrate and dismantle virtual criminal operations.

The third "P"—partnerships—means building even stronger relationships with law enforcement agencies worldwide. He said we've worked with such countries as Great Britain, Canada, Russia, and Turkey to swap best practices and techniques. We've also sent agents to Romania to work with law enforcement there, leading to nearly 100 arrests in cyber crime cases representing "tens of millions of dollars" in losses, Henry said.

And the Internet Crime Complaint Center, or IC3—a partnership between the FBI and the National White Collar Crime Center—continues to assist state and local law enforcement in fighting cyber crime. Since its establishment in 2000, IC3 has received more than a million complaints. In the last couple of years, there's been an "uptick" in the number of reports, according to Henry. Lately, they're coming in at the rate of nearly 20,000 per month.

Resources:
- More about IC3
- FBI stories about cyber crime

Headline Archives home