

advertisement



Bouquets \$19.99 +s/h

Send flowers for any occasion from

ProFlowers

Offer ONLY available at:  
[proflowers.com/happy](http://proflowers.com/happy)  
or call 1.877.804.1133

 **msnbc.com**

## U.S. sees cyber arrests leading to more hackers

Officials call FBI crackdown on Anonymous a deterrent, but some experts skeptical

By **Jeremy Pelofsky**

 **REUTERS**

updated 7/21/2011 7:20:49 PM ET

**WASHINGTON**— The FBI's arrest this week of 16 people who allegedly participated in high-profile cyber attacks is providing a treasure trove of information and will lead to further arrests, a U.S. law enforcement official told Reuters Thursday.

The crackdown — on members of the group Anonymous — was the biggest reaction so far by U.S. authorities to a string of cyber attacks, and was meant to serve as a deterrent to others who may be considering joining the cause.

The arrests spanned nine states and the District of Columbia. FBI agents also executed more than 35 search warrants, seizing computers and other records. Those arrested could try to strike plea agreements offering to provide information to win more lenient treatment.

Some private cyber security specialists have questioned whether the raids will have much lasting impact.

But the law enforcement official said, "This is

successfully removed a number of individuals from being part of the problem and will certainly lead to information that will result in locating other subjects." The official declined to be further identified while speaking about an ongoing law enforcement investigation.

Members of Anonymous mounted attacks last year against eBay's PayPal as well as Visa and Mastercard after the companies severed their relationships with the WikiLeaks organization. The attacks included flooding the sites with data trying to render them inoperable.

The arrests included members of Anonymous at various levels of the loose-knit organization, the official said. The official declined to comment on whether they knew each other.

While attacks by Anonymous and related "hacktivist" groups have drawn wide attention, other cyber crimes aimed at espionage are a higher priority for the FBI. The latter have included intrusions at Google, Lockheed Martin and the International Monetary Fund.

"We didn't pull resources away from those higher priority cases to work this," the official said.

It remains an open question whether the

Print Powered By  **FormatDynamics™**



Security, issued a statement Thursday saying they would continue their efforts.

"I think they (the FBI) are trying to send a signal that this isn't cost-free in the hopes that it will scare off some of the others. If we're lucky it will work," said James Lewis, a cyber security expert with the Center for Strategic and International Studies think tank.

The law enforcement official said that people allegedly involved in the cyber attacks probably did not realize the risks of prison time and that prosecutors would likely seek stiff sentences. Those arrested, if convicted, could face up to 10 years in prison for trying to damage a protected computer.

"They're probably not the types of people who have been prepared for any time in jail. This is not a joke," the official said. "The reality of the fact that this is both a crime and that people will be actually doing time in jail I think really hasn't sunk in to a lot of people who are getting involved in these activities."

Lewis said one possible benefit from the cyber attacks is that it will lead network and website administrators to beef up their security.

"These guys exploit poor configuration, and that's the simplest thing to fix but there's just so much of it out there it will take a while,"

*Copyright 2011 Thomson Reuters. [Click for restrictions.](#)*

Sponsored links

Print Powered By  FormatDynamics™