From www.infect.com <http://www.infect.com/>

Web Sites Hawk Instructions On Making Computer Viruses;
Why FBI's Hands Are Tied

By CASSELL BRYAN-LOW and GARY FIELDS
Staff Reporters of THE WALL STREET JOURNAL
March 31, 2005; Page B1

The Web site of American Eagle Publications Inc. has a provocative come-on for the CDs it sells. "The software on this CD-ROM is responsible for having caused literally billions of dollars of damage," goes the teaser for one.

The CD in question, called "Outlaws of the Wild West" and priced at $49.95, contains the source code -- the equivalent of a recipe -- for 14,000 types of viruses, according to the Web site. It also includes virus-writing tools, newsletters about "destructive code" and a database describing how different viruses work.

American Eagle Publications, whose site is registered in Show Low, Ariz., is just one of a number of small, controversial online retailers that hawk do-it-yourself virus kits. Many Web sites even make virus recipes available at no charge.

At a time of mounting public concern about identity theft, "phishing" and other forms of electronic crime, computer-security experts complain that the increasingly brazen proliferation of virus-writing guides is destructive. But, they add, there is little law-enforcement officials can do to fight back.

The reason lies in the law: Publishing source code that can be used to construct viruses isn't illegal. What is illegal, according to the U.S. Computer Fraud and Abuse Act of 1986, is to release a virus with the knowledge that it will harm others. The distinction, lawyers say, is akin to gun ownership: Owning a gun usually isn't illegal in the U.S. unless you use it to kill or rob someone. Thus, virus purveyors aren't feeling much heat.

"There's nothing illegal about putting the code to viruses on the Internet," says Federal Bureau of Investigation special agent Jeff Lanza. The First Amendment right to free speech, he says, means there is nothing that the agency has done or can do to change the law in this area.

It is "extremely frustrating," adds Mr. Lanza. "We have enough people sending viruses through the Net that know how to do it. We don't need neophytes handed a turnkey operations guide."

There are, of course, efforts under way to crack down on Internet vandalism. Companies such as Microsoft Corp. are scrambling to patch the vulnerabilities in their software, and law-enforcement agencies around the globe are stepping up their fight against cyber crooks. In January, a federal judge in the state of Washington sentenced 19-year-old Jeffrey Lee Parson to 18 months in prison for spreading a variant of the so-called Blaster worm, which surfaced in 2003 and shut down computers running Microsoft Windows. But vandals aren't the only worry: Viruses are increasingly being employed as tools for identity theft and to commandeer computers to pump out e-mails hawking pirated goods.

Mr. Lanza says the FBI is aware of some sites that make virus code available but doesn't monitor them. A site may fall under an FBI investigation if a virus unleashed on the Internet is traced back to that site. But even then, he says, you can't hold someone criminally responsible simply for putting the virus recipe into the public domain where others might pick it up.

To make a case that sticks, prosecutors need to prove that a suspect is guilty of intentionally damaging others' computers -- which is what Mr. Parson was found guilty of doing. The government could also potentially prosecute people for posting code if the sites encourage using the viruses to cause harm. But legal experts say building such cases is difficult because prosecutors need to show that the accused was advocating a specific unlawful activity, such as infecting a particular computer.

Still, for security experts like Ken Dunham, a virus specialist at information-security consultant iDefense Inc. of Reston, Va., the unfettered distribution of viruses "is troublesome." Such sites "provide hackers with the tool of the trade and greatly encourage new actors to get involved."

Even well-intentioned efforts by security researchers -- who sometimes publish virus code themselves to demonstrate potential weaknesses in software -- quickly get exploited by people with nefarious intentions, says Stephen Toulouse, a security specialist at Microsoft.

Marc Zwillinger, a former Department of Justice attorney and currently a partner at Sonnenschein Nath & Rosenthal LLP in Washington, D.C., says law-enforcement officials have discussed whether to push for legislation that would criminalize virus-writing tools. "The problem is that some of the same tools have very legitimate use in the security profession," he says, such as in testing the security of computer systems. For that reason, law enforcement has focused on legislation that makes the activity -- not the technology -- illegal.

For its part, American Eagle Publications acknowledges -- indeed, revels in -- the controversial nature of its wares. "People have gone to jail for writing it," the site says of the contents of its "Outlaws of the Wild West Computer Virus CD-ROM."

But the site argues the CDs it sells are protected under the right to free speech. Among other items it offers is an eclectic list of books, including "Storm Over Show Low," a conservative thriller in which patriotic denizens of the Arizona town fight for their rights against growing government control. The site is registered to Mark Ludwig, the author of several books on viruses. Mr. Ludwig couldn't be reached to comment.

A spokeswoman for the U.S. attorney's office in Arizona declined to comment.

Security experts say it's difficult to estimate how much virus information is sold or distributed online. The code for sale ranges from the out-of-date to the highly sophisticated. But CDs similar to the one sold by American Eagle can be found at a host of small online software retailers, at prices ranging from $15 to $50 per title. A simple Internet search turned up numerous sites selling titles like "Hacker Toolbox," "Master Hacker " and "Virus Creation Lab."

Virus Creation Lab is among the CDs for sale at a site called Beahacker.com. The site's catalog also includes a "Guide to Hacking" CD, which promises tutorials on "email bombs" and "hard drive killers."

That CD also offers how-to information on "keyboard loggers,"programs that capture people's keystrokes as they enter them. These have become popular with identity thieves, who steal credit-card and other financial data.

In an e-mail response to questions about its wares, Beahacker.com's administrator said the merchandise is for people who want to test the security of their computer systems. "We notify all clients that we cannot sell the products if they will use the products to commit crimes," said the administrator, who identified himself as Andy Hooda, a 29-year-old Chicago resident and owner of the site.

Among Web sites that make code available free of charge is that of a virus-writing group called 29A. With members in Europe, Russia and Brazil, 29A is notorious in computer-security circles for creating innovative viruses. The group claims that it writes them for the academic challenge of it and generally opposes releasing them. But its site says it doesn't forbid its members from spreading viruses.

Asked how the group responds to those who say it is irresponsible to make viruses easily available, a 29A member from Spain who goes by the nickname "VirusBuster" said in an e-mail:

"We ignore them."