August 2011
Issue No. 7

U.S. Attorney's Report to the District

Late last month, the National Security Council released a **report** detailing the Government's "Strategy to Combat Transnational Organized Crime." The report recognized that transnational organized crime networks "are increasingly involved in cybercrime, which costs consumers billions of dollars annually, threatens sensitive corporate and government computer networks, and undermines worldwide confidence in the international financial system. . . . Pervasive criminal activity in cyberspace not only directly affects its victims, but can imperil citizens' and businesses' faith in these digital systems, which are critical to our society and economy."

While Connecticut might seem safely distant from the dangers of transnational organized crime, that is unfortunately not the case. Law enforcement agencies in Connecticut, including the FBI, the Secret Service, and local police departments, are routinely called upon to investigate computer intrusions perpetrated from overseas, as well as money stolen and sent overseas from online bank accounts of victims—individuals and businesses—located here in Connecticut.

Over the past several months, we have taken a significant step in striking back against international cybercriminals by dismantling the Coreflood "botnet." A botnet is a collection of computers infected with a virus—in this case, the Coreflood virus—which can be used by criminals to exercise complete control over infected computers. Coreflood is known to have infected millions of computers around the world, including thousands of computers here in Connecticut. Coreflood was used to steal private personal and financial information from the infected computers, such as online banking credentials. The stolen information was then used to initiate fraudulent wire transfers from the victims' bank accounts.

In April, the FBI, the United States Marshals Service, and the United States Attorney's Office commenced Operation Adeona. The operation—which was the most comprehensive of its kind anywhere—involved a three-pronged effort to dismantle the Coreflood botnet. First, law enforcement authorities seized control of the Coreflood botnet, in order to prevent Coreflood from continuing to steal data from infected computers. Second, with the assistance of all major Internet service providers, the owners of infected computers were given notice of the Coreflood infection and given instructions on removing Coreflood. Finally, law enforcement authorities worked closely with anti-virus software vendors to ensure that their anti-virus software would be

effective against the latest versions of Coreflood. By the time the operation came to a close in June, the Coreflood botnet had been decimated and no longer posed a threat. The operation demonstrated the technical prowess of our law enforcement agencies in Connecticut and exemplified the superb results that can be achieved when public sector and private sector entities work together.

I am often asked by concerned citizens how to avoid becoming victims of computer crime. There is, unfortunately, no easy answer to that question, because of the many different types of computer crime and the ever-increasing sophistication of cyber-criminals. The United States Attorney's Office has successfully prosecuted recent cases involving fraudsters, "phishers," and identity thieves, to name just a few. There is a great deal of information about these types of crimes, and how to avoid falling victim to them, on the Internet sites of the FBI (click **here**), the Federal Trade Commission (click **here**), and the Internet Crime Complaint Center (click **here**). Beyond that, I would urge everybody using a computer on the Internet to install reputable anti-virus software and to keep that software, and all other software on their computers, properly updated. By taking those simple steps, we can make crime significantly harder to commit for cyber-criminals around the world.