Attorneys:

- **Timothy G. Ronan**
  tronan@pullcom.com
  203.674.7933

CYBER LAW TRACKER: April 2011

The Latest in Cybersecurity and Infrastructure Protection Legal Developments

U.S. ATTORNEY'S OFFICE FOR THE DISTRICT OF CONNECTICUT FILES CIVIL ACTION AGAINST "JOHN DOE" DEFENDANTS SEEKING AUTHORIZATION TO SEIZE CONTROL OF COREFLOOD BOTNET

by T. Scott Cowperthwait, Posted on April 14, 2011

On April 12, 2011, the U.S. Attorney's Office for the District of Connecticut initiated a civil action against 13 "John Doe" defendants with respect to a malicious software program, known as "Coreflood," which steals data from infected computers. The complaint charges the "John Doe" defendants with wire fraud (18 U.S.C. § 1343), bank fraud (18 U.S.C. § 1344) and unauthorized interception of electronic communications (18 U.S.C. § 2511) based on a scheme involving the use of Coreflood to obtain surreptitious and unauthorized access to computers throughout the United States.

According to papers filed with the Court, the "John Doe" defendants and their co-conspirators use Coreflood to record keystrokes and Internet communications, including usernames, passwords and other private personal and financial information, and then extract online banking information credentials and other information. They then use the stolen information to direct fraudulent wire transfers to themselves from the bank accounts of their victims.

Earlier this month, the government obtained search and seizure warrants authorizing the seizure of all known Coreflood command and control servers and associated Internet domain names. While the seizure of the servers and domain names breaks the "John Doe" defendants' control over the infected computers, it does not stop Coreflood from continuing to gather information from infected computers. In an effort to address this gap, the government has requested the issuance of a restraining order and injunction which would authorize the

government to establish a substitute server operated under law enforcement supervision by the non-profit Internet Systems Consortium. The substitute server would continue to communicate with infected computers located in the United States and send commands to those computers directing Coreflood to stop running, thus disabling the malicious software program. The Court has scheduled a hearing for April 25, 2011, on this matter.

Stay tuned for further alerts concerning issues relating to this first of its type enforcement action.