Judge lets US intercept info from hacked computers (Update)

June 3 2014, by Joe Mandak

The Justice Department can continue to intercept information from 350,000 computers worldwide that are known to be infected with a data-stealing virus being spread by an alleged Russian computer hacker and his conspirators, a federal judge said.

Justice Department attorneys told U.S. District Judge Arthur Schwab the affected computers will remain linked to a government-provided substitute Internet server until the malicious software can be removed. The substitute server lets the government track the Internet addresses of the infected computers and pass them on to Internet service providers or government agencies in countries, so that computer-owners can be alerted to infections.

The hackers are allegedly led by a 30-year-old Russian man, Evgeniy Bogachev, who is not in custody. The hackers infected computers with a piece of malicious software that captured bank information used to drain more than $100 million from accounts or another that locked computer files until ransom payments were made.

Tuesday's hearing on the preliminary injunction was held in Pittsburgh, where the Justice Department has charged Bogachev with siphoning more than $370,000 from a western Pennsylvania plastics firm using the virus known as Gameover Zeus.

The injunction issued Tuesday extends a temporary order the judge issued last week when Justice Department attorneys notified the court of

the scam in sealed documents.

Since then, the government has moved to seize key computer servers in Canada, Ukraine and Kazakhstan, which were used to spread the ransom-demanding virus known as Cryptolocker. Victims included the Swansea, Massachusetts, police department, which paid a $750 ransom using the virtual currency Bitcoin to unlock its computer files.

Other businesses, including an eastern Pennsylvania assisted living company and a North Carolina pest control firm, paid $70,000 and $80,000, respectively, to have employees or computer experts fix their Cryptolocker-infected computers.

Schwab issued his order based on a 28-page report filed by a Pittsburgh FBI computer expert, Special Agent Elliott Peterson. Among other things, the report says 230,000 computers had been infected by Cryptolocker since mid-2013, including 120,000 in the United States. It's unknown how many of those computer owners paid ransoms to unlock their files, the report said.

The Cryptolocker servers have been "dismantled," Justice Department attorney Ethan Arenson told the judge.

Additionally, "350,000 infected computers have been liberated from the Gameover Zeus botnet"—an automated network spawned by the data-stealing virus—by connecting them to the government's substitute server, Arenson said.

Those computer owners can get help removing the malicious software at a website maintained by the Department of Homeland Security, www.us-cert.gov/gameoverzeus.

Judge Schwab granted the injunction after no one representing Bogachev

or the other alleged hackers appeared in court to contest it. The judge ordered the government attorneys to file a report by July 11 to update the progress being made to fix infected computers.