Updated Alert

Prepared by the
Internet Crime Complaint Center (IC3)
August 09, 2012

CITADEL MALWARE CONTINUES TO DELIVER REVETON RANSOMWARE IN ATTEMPTS TO EXTORT MONEY

The IC3 has been made aware of a new Citadel malware platform used to deliver ransomware, named Reveton. The ransomware lures the victim to a drive-by download website, at which time the ransomware is installed on the user's computer. Once installed, the computer freezes and a screen is displayed warning the user they have violated United States Federal Law. The message further declares the user's IP address was identified by the Federal Bureau of Investigation as visiting child pornography and other illegal content.

To unlock the computer, the user is instructed to pay a fine to the US Department of Justice, using prepaid money card services. The geographic location of the user's IP address determines what payment services are offered. In addition to the ransomware, the Citadel malware continues to operate on the compromised computer and can be used to commit online banking and credit card fraud.

Below is a screenshot of one variation of the warning screen.

This is an attempt to extort money with the additional possibility of the victim's computer being used to participate in online bank fraud. If you have received this or something similar do not follow payment instructions. Infected computers may not operate normally. If your computer is infected, you may need to contact a local computer expert for assistance to remove the malware.

It is suggested that you;

- File a complaint at www.IC3.gov.
- Seek out a local computer expert to assist with removing the malware.