Citadel Malware Continues to Deliver Reveton Ransomware in Attempts to Extort Money

In early August, the FBI reported continuing rise in the use 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 has been identified by the Federal Bureau of Investigation as visiting websites that feature child pornography and other illegal content.

To unlock the computer, the user is instructed to pay a fine to the U.S. Department of Justice using a prepaid money card service. 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.

The FBI reports that 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 CU members receive this communication or something similar, do not follow payment instructions. Infected computers may not operate normally and if your computer is infected, you may need to contact a local computer expert for assistance to remove the malware.

The FBI suggests you:

- Do not pay any money or provide any personal information.
- Be aware that even if you are able to unfreeze your computer on your own, the malware may still operate in the background. Certain types of malware have been known to capture personal information such as user names, passwords, and credit card numbers through embedded keystroke logging programs.
- If you feel your computer has been infected, you should consider contacting a local computer expert to assist with removing the Citadel malware and Reveton.
- File a complaint at www.IC3.gov if you receive any information noted above, and look for updates about the Reveton virus on the IC3 website.