Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

November 30, 2012

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

A new extortion technique is being deployed by cyber-criminals using the Citadel malware platform to deliver Reveton ransomware. The latest version of the ransomware uses the name of the Internet Crime Complaint Center to frighten victims into sending money to the perpetrators. In addition to instilling a fear of prosecution, this version of the malware also claims that the user's computer activity is being recorded using audio, video, and other devices.

As described in prior alerts on this malware, it 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 that a law enforcement agency has determined that a computer using the victim's IP address has accessed child pornography and other illegal content.

To unlock the computer, the user is instructed to pay a fine using prepaid money card services. The geographic location of the user's PC 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 the new variation.

This is not a legitimate communication from the IC3, but rather is an attempt to extort money from the victim. If you have received this or something similar do not follow payment instruction.

It is suggested that you:

- File a complaint at www.IC3.gov.
- Keep operating systems and legitimate antivirus and antispyware software updated.
- Contact a reputable computer expert to assist with removing the malware.