Updated Alert

Prepared by the
Internet Crime Complaint Center (IC3)
July 29, 2012

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

The Federal Bureau of Investigation's Internet Crime Complaint Center (IC3) and the Department of Homeland Security (DHS) have recently received complaints regarding a ransomware campaign using the name of the DHS to extort money from unsuspecting victims.

In May 2012, the IC3 posted an alert about the Citadel malware platform used to deliver ransomware known as Reveton. The ransomware directs victims to a download website, at which time it is installed on their computers. Ransomware is used to intimidate victims into paying a fine to "unlock" their computers. The ransomware has been called "FBI Ransomware" because it frequently uses the FBI's name including the names of FBI programs such as InfraGard and IC3. Similar ransomware campaigns have used the names of other law enforcement agencies such as the DHS.

As in other variations, the ransomware using the name of the DHS produces a warning that accuses victims of violating various U.S. laws and locks their computers. To unlock their computers and avoid legal issues, victims are told they must pay a $300 fine via a prepaid money card.

This is not a legitimate communication from law enforcement, but rather is an attempt to extort money from the victim. If you have received this or something similar, do not follow the instructions in the warning and do not attempt to pay the fine.

It is suggested that you;

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