

## FBI – Malware attempting to extort money

Victims are being lured to an Internet site that installs ‘ransomware’ on their computer. The ransomware freezes the computer, declares the user’s computer has been identified as visiting a child porn site ( or site with other illegal content) and displays a screen that US Federal law has been violated.

To unfreeze the computer, the user is instructed to pay a \$100 fine. Even though the computer is unlocked when the ‘fine’ is paid, the malware continues to operate and can be used to commit online banking fraud and credit card fraud (which is how the fine was probably paid!)

If you have received this or something similar, **do not follow payment instructions.**

It is suggested that you:

- Contact your banking institutions.
- File a complaint at [www.IC3.gov](http://www.IC3.gov).

(Nothing was said how to unlock the computer without paying)

Read on to learn more.

.....

### **Citadel Malware Delivers Reveton Ransomware in Attempts to Extort Money**

05/30/12—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 Computer Crime & Intellectual Property Section as visiting child pornography and other illegal content.

To unlock the computer, the user is instructed to pay a \$100 fine to the U.S. 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.

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.

It is suggested that you:

- Contact your banking institutions.
- File a complaint at [www.IC3.gov](http://www.IC3.gov).