



COT Security Alert – FBI.Cybercrime Division Ransomware

The COT Security Administration Branch has been informed of a ransomware infecting state-owned computers. Ransomware locks the user's system and delivers a pop-up that demands money to unlock the system. The malware delivered to lock the system infects it so that rebooting and other efforts to recover are useless. Sending the money is not an option, since scammers are not truly concerned to unlock the user's system.

In this case, the ransomware says it is from the FBI, but is actually from an unknown third party. The user likely becomes infected by simply visiting an infected website in what is called a "drive-by" infection. The pop-up states you have infringed copyright laws or some other crime and must pay a fine to recover use of your computer. The FBI never operates in this manner. This particular ransomware infection was first reported to the FBI in August of 2012, but as with all malware new versions are created to avoid detection by antivirus software.

FBI site:

<http://www.fbi.gov/news/stories/2012/august/new-internet-scam/>

Users who become infected should not attempt any kind of recovery, but should report the incident to their IT support immediately. The tactic used has changed over time and this infection or one like it may come in many forms. Any demand for money to unlock a computer system should be reported.

NOTICE: COT is providing this information so that you are aware of the latest security threats, vulnerabilities, software patches, etc. You should consult with your network administrator or other technical resources to ensure that the appropriate actions for these alerts are followed. If you are a network administrator and need additional information, please call the Help Desk at 502.564.7576.

Security Administration Branch
Commonwealth Office of Technology
120 Glenn's Creek Road, Jones Building
Frankfort, KY 40601
COTSecurityServicesISS@ky.gov
<http://technology.ky.gov/CISO/>