Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

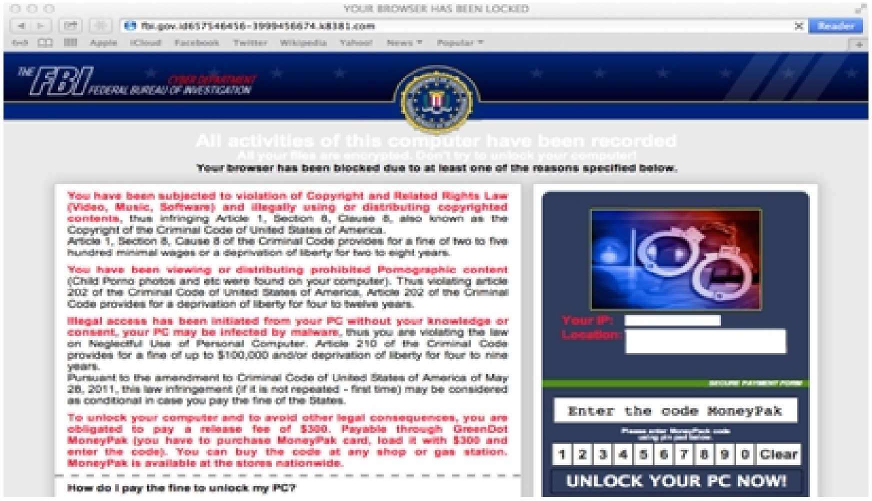
July 18, 2013

RANSOMWARE PURPORTING TO BE FROM THE FBI IS TARGETING OS X MAC USERS

In May 2012, the Internet Crime Complaint Center posted an alert about the Citadel malware platform used to deliver ransomware known as Reveton. The ransomware directs victims to a drive-by 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. Paying the fine does nothing to solve the problem with the computer; do not follow the ransomware instructions. The ransomware has been called "FBI Ransomware" because it uses the FBI's name.

The newest version of ransomware targets OS X Mac users. This new version is not a malware; it appears as a webpage that uses JavaScript to load numerous iframes (browser windows) and requires victims to close each iframe. The cyber criminals anticipate victims will pay the requested ransom before realizing all iframes need to be closed.

The ransomware is pushed to victims' computers when they browse common websites, specifically when they query popular search terms. Once the web browser is exploited, the victims' computer displays a pop-up warning that appears to be from the FBI. Cyber criminals use "FBI.gov" within the URL to make the warning appear more legitimate.


YOUR BROWSER HAS BEEN LOCKED
fbi.gov.id6575446456-3999456674.k8381.com
Reader
Apple
iCloud
Facebook
Twitter
Wikipedia
Yahoo!
News
Popular
THE FBI
CYBER DEPARTMENT
FEDERAL BUREAU OF INVESTIGATION

All activities of this computer have been recorded

All your files are encrypted. Don't try to unlock your computer!

Your browser has been blocked due to at least one of the reasons specified below.

You have been subjected to violation of Copyright and Related Rights Law (Video, Music, Software) and illegally using or distributing copyrighted contents, thus infringing Article 1, Section 8, Clause 8, also known as the Copyright of the Criminal Code of United States of America.
Article 1, Section 8, Cause 8 of the Criminal Code provides for a fine of two to five hundred minimal wages or a deprivation of liberty for two to eight years.

You have been viewing or distributing prohibited Pornographic content (Child Porno photos and etc were found on your computer). Thus violating article 202 of the Criminal Code of United States of America, Article 202 of the Criminal Code provides for a deprivation of liberty for four to twelve years.

Illegal access has been initiated from your PC without your knowledge or consent, your PC may be infected by malware, thus you are violating the law on Neglectful Use of Personal Computer. Article 210 of the Criminal Code provides for a fine of up to $100,000 and/or deprivation of liberty for four to nine years.
Pursuant to the amendment to Criminal Code of United States of America of May 28, 2011, this law infringement (if it is not repeated - first time) may be considered as conditional in case you pay the fine of the States.

To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of $300. Payable through GreenDot MoneyPak (you have to purchase MoneyPak card, load it with $300 and enter the code). You can buy the code at any shop or gas station. MoneyPak is available at the stores nationwide.

How do I pay the fine to unlock my PC?

Your IP:

Location:

SECURE PAYMENT FORM
Enter the code MoneyPak
Please enter MoneyPack code using pin pad below.
1 2 3 4 5 6 7 8 9 0 Clear
UNLOCK YOUR PC NOW!

Malwarebytes Unpacked – Jerome Segura

As the FBI saw in 2012, the warning accuses victims of violating various U.S. laws and locks their computer. To unlock the computer and avoid legal issues, victims are told they must pay a $300 fine via a prepaid money card. Attempts to close the warning page results in additional messages that reappear each time victims try to close their web browser.

The simplest way to remove the ransomware's iframes is by clicking on the Safari menu and choosing "reset Safari," make sure all check boxes are selected, or hold down the Shift key while relaunching Safari. This will prevent Safari from reopening windows and tabs from the previous session. Victims

	can also disable the reopening feature across OS X from the General pane of System Preferences. Ransomware messages are an attempt to extort money. If you have received a ransomware message do not follow payment instructions and file a complaint at https://www.ic3.gov/