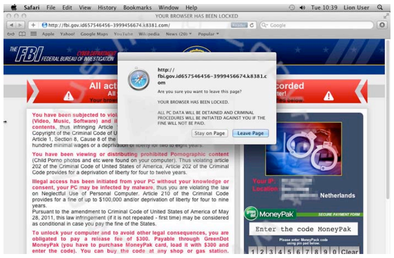
Ransomware...Data Pirates Move Down The Food Chain....

Data Pirates have decided its much easier pickings to get $500 bucks from lots of individuals than the harder job of hacking larger more "protected" companies.


Safari File Edit View History Bookmarks Window Help
Tue 10:39 Lion User
YOUR BROWSER HAS BEEN LOCKED
http://fbi.gov.id657546456-3999456674.k8381.com/
Reader
Google
Apple Yahoo! Google Maps YouTube Wikipedia News (20) Popular
THE FBI FEDERAL BUREAU OF INVESTIGATION
CYBER DEPARTMENT
All act
All
Your brow
corded
ter!
fied below.
Stay on Page
Leave Page
MoneyPak
SECURE PAYMENT FORM
1 2 3 4 5 6 7 8 9 0 Clear

http://
fbi.gov.id657546456-3999456674.k8381.com

Are you sure you want to leave this page?

YOUR BROWSER HAS BEEN LOCKED.

ALL PC DATA WILL BE DETAINED AND CRIMINAL PROCEDURES WILL BE INITIATED AGAINST YOU IF THE FINE WILL NOT BE PAID.

You have been subjected to viol (Video, Music, Software) and il contents, thus infringing Article Copyright of the Criminal Code of U Article 1, Section 8, Cause 8 of the 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.

Your IP: [redacted]
Location: [redacted] Netherlands

Enter the code MoneyPak

Please enter MoneyPack code using pin pad below.

Recent hostage situations include Hollywood Presbyterian Medical Center, initial demand $3.4 million and Police departments in Maine and Mass for between $300 and $500. What’s the similarity in attack?

So, it’s all a variation on phishing. That innocuous email that looks like its from a friend/known business associate that when you "click" on the file infects your device/system with the malware that leads to all your files being frozen and a ransomware demand.

Many individuals are also getting these kind of attacks with similar demands. So what happens next?

Well, you can run down to the Geek Squad or your local PC guy for advice or check out the FBI or other sites that offer code to "unlock" the malware but inevitably the same question is first asked, "Did you have all your system backed up?" They ask this for a simple reason, you're whole device may need to be wiped if it can't be unlocked and you're whole system may need to be wiped if the Pirate doesn't unlock your system after you've paid the ransom!!!!

Can you cope with that loss of all your data??

What can we do to safeguard and mitigate against this ?

- We need to back up our systems regularly, externally and in the safest place we can find.
- We need to make sure we are regularly taking in new "patches" and updates to software
- We need to re-check and update firewalls
- We need to educate ourselves and employees about the dangers of phishing emails and their effect
- We need to be ever alert and diligent

This problem isn't going away and whether its our business data or our PII the effects can be devastating.

We'll be publishing a white paper on this subject soon so stay tuned.......

WWW.IDRESOLUTION.NET