

Forum:[Hack Forums](#)

Thread: [Some kind of police virus?](#)

BlondeMan - September 27, 2013, 1:45 pm

Hi, i think i'm infected with a virus.

When i try to connect to my computer it tells me that i need to pay 500\$

I have heard about this before, is their anyway i can remove this?

I can't even go to my desktop, the screen gets white and it says " Downloaded Child Porn or something stupid like that :/ "

Edit: I have this virus [Click](#)

L3nn0r1129 - September 27, 2013, 2:31 pm

i also encountered the same problem as yours. to fix it i used hirens boot cd i make a bootable disk and boot it to mini xp of hiren's and i go to program menu of hiren's and run malwarebytes to scan my drives and delete that virus.

imamtaco - September 27, 2013, 3:02 pm

i also had it but mine was 300\$ but for same reason all i did was push the power button on my pc it exited the virus screen and said are you sure you want to power off pc i said no and it was gone,then i removed it buy using malawarebytes.

Blue Hawk - September 27, 2013, 4:18 pm

i did a little research on this virus here is the link it states how to get rid of it and how to restore your pc. if you do not trust link i will post the main info

<http://botcrawl.com/how-to-remove-the-fbi-moneypak-ransomware-virus-fake-fbi-malware-removal/>

info-

The FBI virus, also referred to as the FBI Moneypak virus, Citadel Reveton, and other terms is dangerous malware categorized as ransomware we discovered in 2012 that cyber criminals use in attempt to disguise themselves as the FBI. The FBI virus utilizes Trojan horses (Trojan.Ransomlock.R, reveton) in order to gain access and lock computer systems. The FBI virus practices a variety of unethical tactics, including social engineering in attempt to persuade or scare unsuspecting victims to pay an unnecessary fine by making fraudulent claims that the computer has been involved in illegal activity (downloaded or distributed copyrighted material or viewed child pornography, etc.) and demands a penalty fine of \$100, \$200, \$300, or more to be paid in order to unlock the computer system within the allotted time of 48 to 72 hours by use of Moneypak cards (REloadit virus, Ultimate Game Card Virus, Ukash Virus). The FBI Moneypak ransomware virus also states on the fake FBI screen that the computer owner may see jail time or face other consequences if the unnecessary fine is not paid in time.

how to remove-

Victims of the FBI Moneypak virus and other forms of ransomware will require separate removal steps due to the progress of the infection. Since this is the case, we have outlined easy options to remove FBI Moneypak malware for all victims. Remove the FBI virus immediately using the options provided in this article by clicking a link below.

Malware Removal Software – Automatically detect and and remove the FBI virus

Manual Removal (Advanced) – Remove associated files

System Restore (Windows) Refresh/Reset (Windows 8) – Restore PC to a date and time before ransomware infection (includes different access options)

Safe Mode With Networking (Troubleshooting) – Manually remove files and/or scan and remove malware (reset proxy settings if needed)

Flash Drive Option – Load Antivirus (or AM) software to a flash drive, scan for and remove malware

Optical CD-R Option – Load Antivirus (or AM) software to a Compact Disk (CD), scan for and remove malware

Slave Hard Disk Drive Option – Scan for and remove malware

Removal Tips-

The safest option to remove the FBI Money Pak virus by using Malwarebytes Anti-Malware software (free or paid versions), AVG, and Norton all of which have been documented to scan and remove FBI Money Pak virus (Citadel Reveton). If you can not connect to the internet but can access your desktop in “safemode” (detailed below) and install Malwarebytes (or AVG, Norton), then proceed to scan and remove the FBI Money Pak virus. If Anti Malware software is malfunctioning proceed to the “Safe Mode With Networking” option in order to correctly perform a scan or install troubleshoot software. Restoring your computer is also an easy and fast solution but may not be suitable for everyone’s needs as you will need to restore your operating system to a restore point that was created (automatically by Windows) before any signs of infection. Restoring your system can lead to the loss of recently installed applications as well (not images, documents, etc). Microsoft suggests to follow the 4th option which is to enter your computer system in safe mode with networking to scan for and remove the virus, and also suggest if internet access is compromised to reset proxy settings. We have provided all steps to do this.

*Logging in as a different user

In most cases if there are multiple accounts on your Windows system you will be able to access the other accounts that are not infected without conflict.

If a second account has administrator rights, in some cases you will be able to remove the infection using this user. To learn more please visit the bottom of this page and view relating forum topics.

Deny flash option

The FBI Money Pak virus utilizes flash and in some cases, disabling (denying) flash can “freeze” the FBI Money Pak virus (suspend), which allows proper removal methods to be performed. Please note this is not a necessity, nor will this remove the virus. This is only an option for specific individual infections. *This may be skipped.

1. To disable (deny) flash visit:

<http://www.macromedia.com/support/documentation/en/flashplayer/help/help09.html>

2. Select the “Deny” radio option

3. Proceed to a removal option: Anti malware software scan and removal or system restore.

What does denying flash do?

If you select Deny, the malicious application does not have access to your camera or your microphone. The application will continue running, but may not function as intended. Alternately, the application may inform you that it can’t continue unless you allow access, in which case you can either allow access or close the application.

Note-

All of this info was provided by

<http://botcrawl.com/how-to-remove-the-fbi-money-pak-ransomware-virus-fake-fbi-malware-removal/>

all i did was look it up,i hope it helps you

Breakbot - September 27, 2013, 4:20 pm

It's called ransomware viruses , just make some searches on google you'll find plenty of tools that can remove it , however make sure you don't fall in fake virus removers

Blue Hawk - September 27, 2013, 4:45 pm

(Sep 27, 2013 04:20 PM)Breakbot Wrote: [\[CITE\]](#) It's called ransomware viruses , just make some searches on google you'll find plenty of tools that can remove it , however make sure you don't fall in fake virus removers

true,also when you find a tool you want to use to remove it with make sure to do some research on that tool so you know what your using,what it will do for you and make sure its not another virus,i would use Malwarebytes anti-Malware though and do a full scan then just remove the viruses it picks up.

bulby13 - September 27, 2013, 6:42 pm

Use HitmanPro.Kickstart and Malwarebytes

HitmanPro.Kickstart

HitmanPro.Kickstart is a program designed to remove ransomware by bypassing the Master Boot Record.

Go on a second computer.

Download HitmanPro.Kickstart from [here](#)

Open the program.

Plug an USB drive.

Click the kick symbol on the bottom.

WARNING!! This will format the USB drive!

Select your USB drive.

Install the software into it.

Unplug it.

With the USB drive, plug it to the infected computer.

On the boot splash screen, go to the BIOS.

In the BIOS, select your USB drive as the boot device.

Now, it will start up.

The ransomware will start up, but within a few seconds, HitmanPro will bypass it.

Do a scan.

If it finds anything, use the 30day trial.

Reboot, then unplug the drive.

Malwarebytes

Malwarebytes is a powerful malware removal tool. It is recommended by lots of people.

Download Malwarebytes from [here](#)

Do a quick scan.

Computer Forensics - September 27, 2013, 11:18 pm

It's a type of a virus that is trying to steal your information by making you pay,p.s don't do that okay,just find some good malware deleting product or just go in safe mode and find the program

Deutscher Fußball-Bund - September 28, 2013, 6:06 am

The moneypak virus strikes again, I feel bad for you man.

KazRow - February 7, 2014, 1:11 pm

Very easy to remove, just boot the PC in safe mode with networking, download Malwarebytes, full scan all drives, and it should be removed. If that doesn't work report back here.

Aura - February 7, 2014, 2:13 pm

(Feb 7, 2014 02:09 PM)decenthacker Wrote: [\[CITE\]](#) this is great post, obviously the develop0er or such virus really hav sense

Please do not gravedig dead threads, thank you.

Gustav. - February 7, 2014, 2:40 pm

(Feb 7, 2014 02:11 PM)KazRow Wrote: [\[CITE\]](#) Very easy to remove, just boot the PC in safe mode with networking, download Malwarebytes, full scan all drives, and it should be removed. If that doesn't work report back here.

Next time, view the date, lol. Threads with 11 replies don't come out of the blue.

iDaNkS - February 8, 2014, 10:29 am

I suggest you use Hiren's Boot CD you can also boot it from USB drive

Aura - February 8, 2014, 10:30 am

(Feb 8, 2014 11:29 AM)iDaNkS Wrote: [\[CITE\]](#) I suggest you use Hiren's Boot CD you can also boot it from USB drive

The thread have been gravediggered, please do not post in it, it's useless.