What is the virus 'FBI MoneyPak' and what to do when attacked by the 'FBI MoneyPak' virus?

If your computer is suddenly locked and you see the message 'Attention! Your computer has been blocked 'and requires you to pay, most likely your computer has been attacked by malware called Trojan Uraus.

If your computer is suddenly locked and you see the message ' *Attention! Your computer has been blocked* 'and requires you to pay, most likely your computer has been attacked by malware called Trojan Uraus.

The FBI MoneyPak virus is 'distributed' through many means. Malicious sites, or legitimate sites have been hacked, and this virus can attack and invade your computer through exploiting kits, using the vulnerability on your computer to install this Trojan. without your permission.

Another way used to 'spread' this malware is to use email spam that is attached to malicious files or links to malicious websites. Cyber-criminals are spam emails that are attached to a fake informational title, tricking you into believing that it is a message from a certain company. And when you are curious, clicking on the link or opening the FBI MoneyPak virus attachment will have the opportunity to attack your computer.

Threats can also be caused by users downloading and installing certain software that they download from the Internet. In the process of installing the software they accidentally installed the malware without knowing it.

Remove the original FBI MoneyPak virus from your computer:

Solution 1: Remove the FBI MoneyPak screen lock virus with System Restore

System Restore will help you restore your computer's system files back to their previous state. It is a way to 'undo' system changes without affecting your personal files, such as e-mail, text.

Because **the FBI MoneyPak virus** will not allow you to start your computer in normal mode, so open **System Restore** in Safe Mode with Command Prompt.

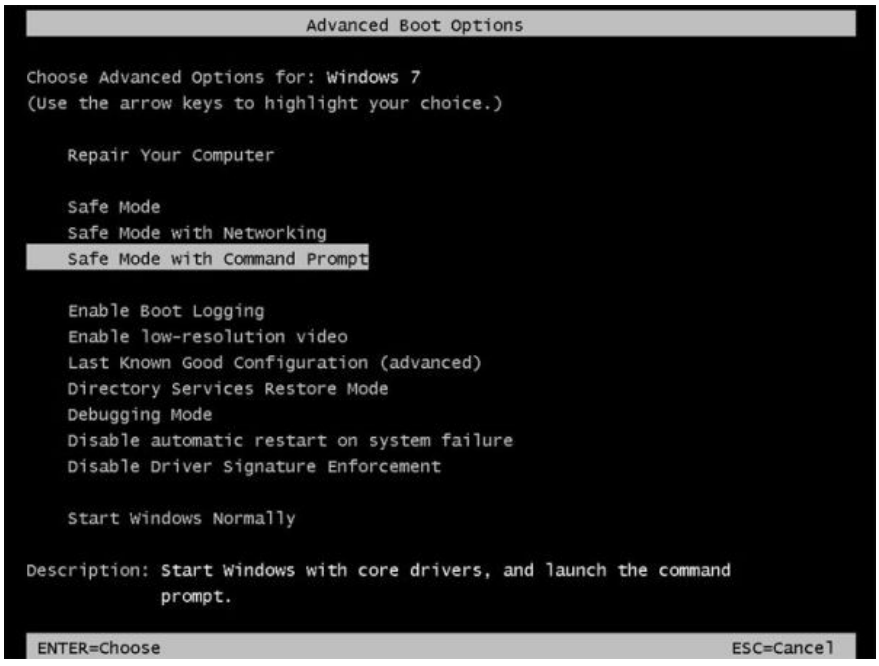
Step 1: Use System Restore to restore Windows to its previous state

1. Start your computer in **Safe Mode with Command Prompt** . To do this, first turn off your Windows computer and then open it again, while your computer starts up, **press the F8 key** before the **Windows logo** appears.

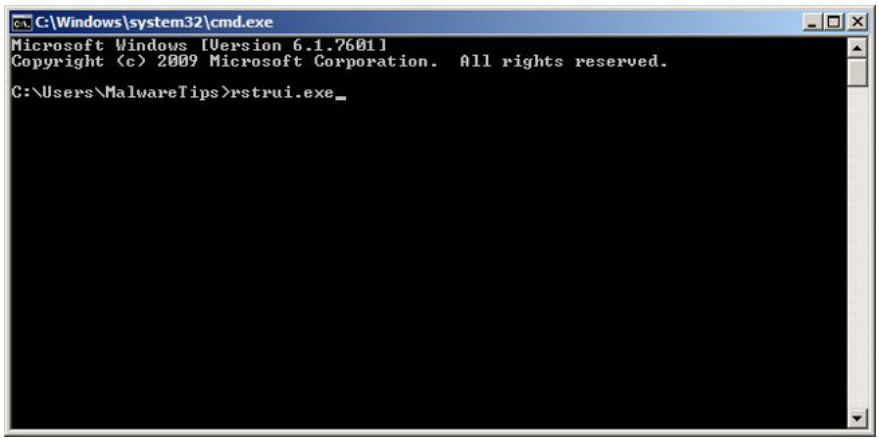
If you're using Windows 8, **press and hold the Shift key** , then **press F8** to boot into Recovery Mode, where you can select recovery options.

On the next screen, find and click the **Troubleshoot** option, then select **Advanced Options** and then select **Windows Startup Settings** . Click the Restart button and you will see the **Advanced Boot Options** window.

2. Use the arrow keys to select **Safe Mode with Command Prompt** and press **Enter** .



3. On the Command Prompt window, type **rstrui.exe** into it and press **Enter** .



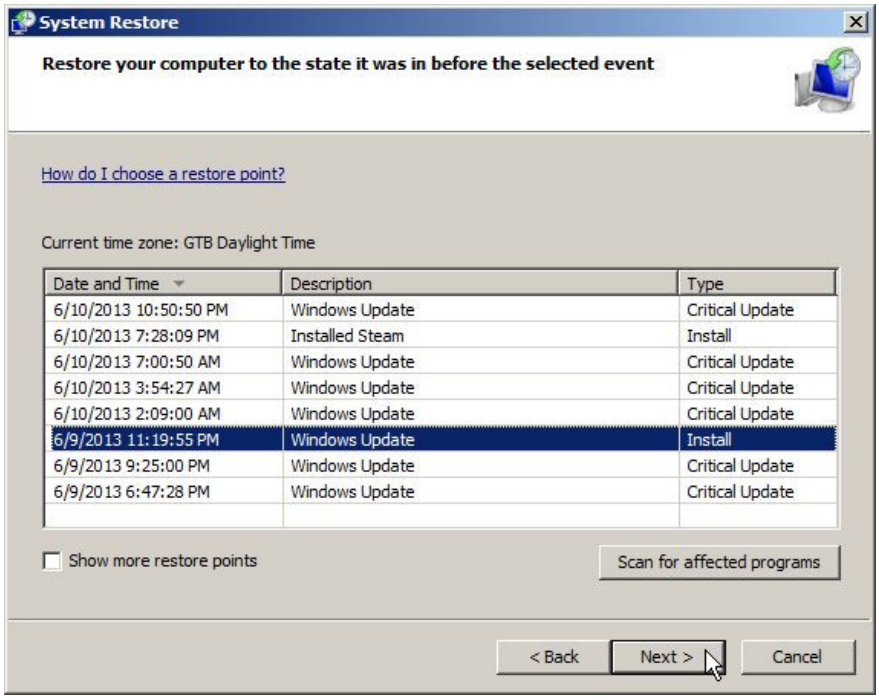
Alternatively, if you are using Windows Vista, Windows 7 and 8, you can enter the following command and press **Enter** :

C: windowssystem32rstrui.exe

If you use Windows XP, enter the command below and press **Enter** :

C: windowssystem32restorerstrui.exe

4. System Restore will open and display on the screen a list of restore points. Try using a restore point at before the **FBI MoneyPak** screen lock virus attacks your computer.



5. When System Restore completes the process, restart your Windows computer in normal mode, then use antivirus software such as **Malwarebytes Anti-Malware** and **HitmanPro** to scan the system again.

Step 2: Use Malwarebytes Anti-Malware Free to remove FBI MoneyPak file

Malwarebytes Anti-Malware is an on-demand system scan tool that will find and remove all traces of malicious software (malware), including worms, Trojans, rootkits, rogues, dialers, spyware (parts Spyware) off your Windows computer.

The important thing is that Malwarebytes Anti-Malware will run in parallel with other antivirus software without conflict.

1. Download Malwarebytes Anti-Malware to your computer and install it.

Download Malwarebytes Anti-Malware to your computer and install it here.

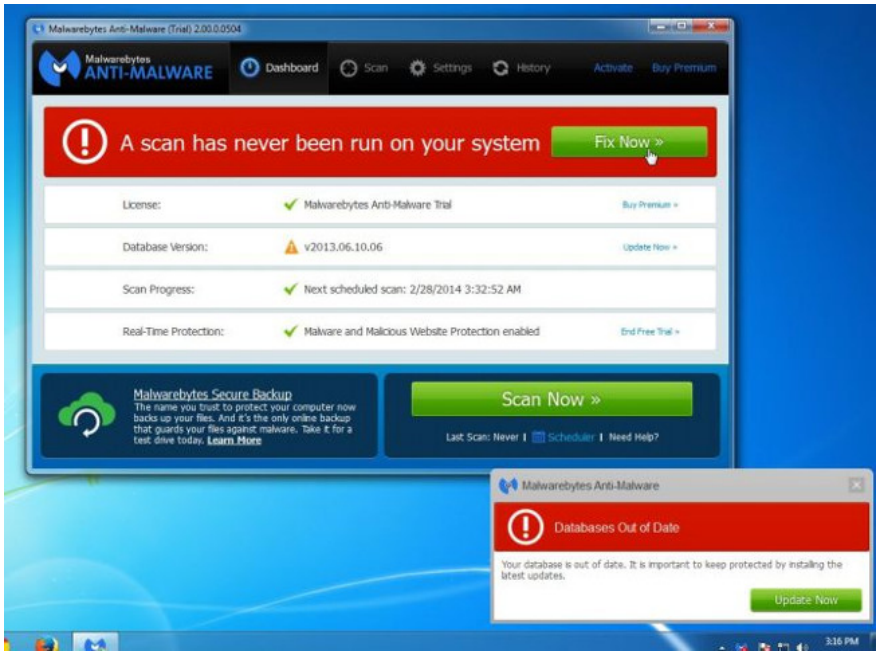
2. After downloading Malwarebytes Anti-Malware, close all programs again, then double click on the icon named **mbam-setup** to start the installation process of Malwarebytes Anti-Malware.

The **User Account Control** dialog box appears now on the screen asking if you want to run the file. Click **Yes** to continue the installation process.

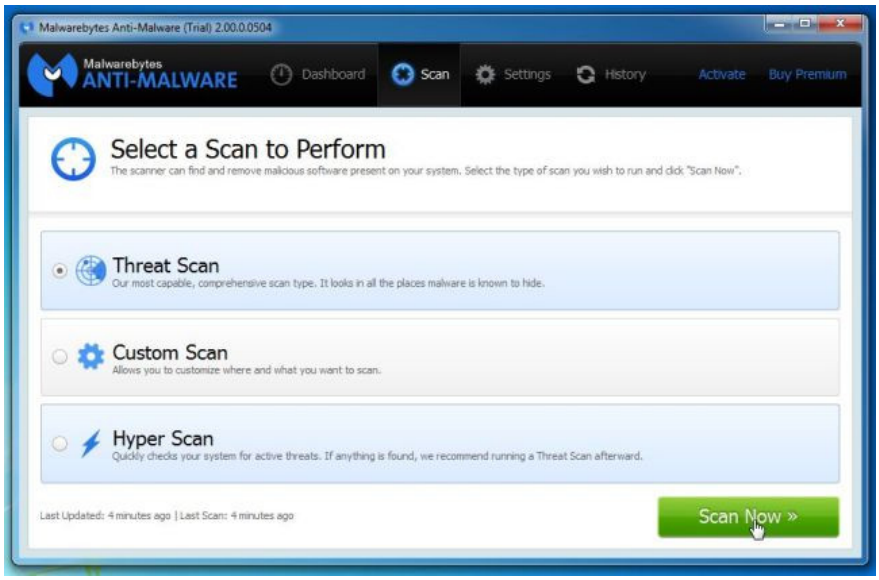
3. Follow the on-screen instructions to install Malwarebytes Anti-Malware Setup Wizard.

Click **Next** to install Malwarebytes Anti-Malware, until the last window click **Finish** to complete.

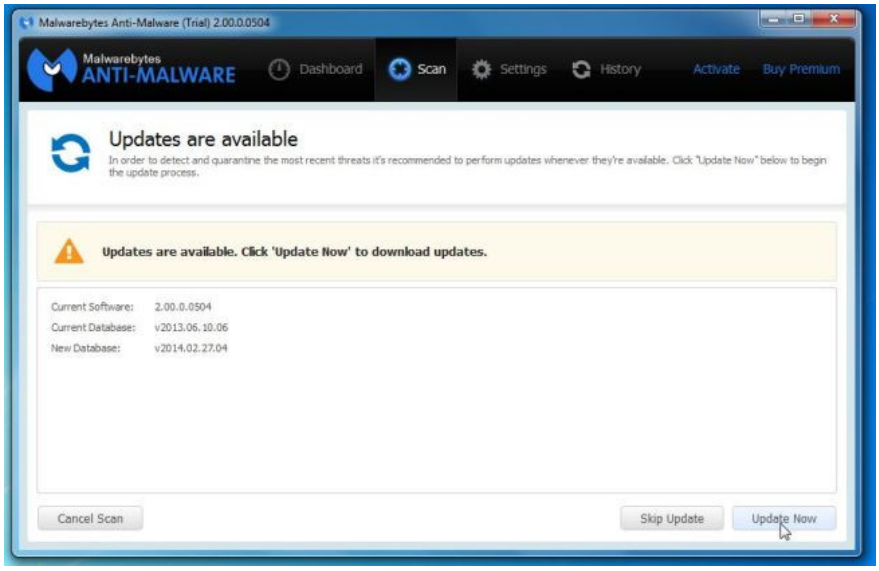
4. After the application has been installed, Malwarebytes Anti-Malware will automatically launch and on the screen you will see a message saying that you should update the program. To start the system scan, click the **Fix Now** button.



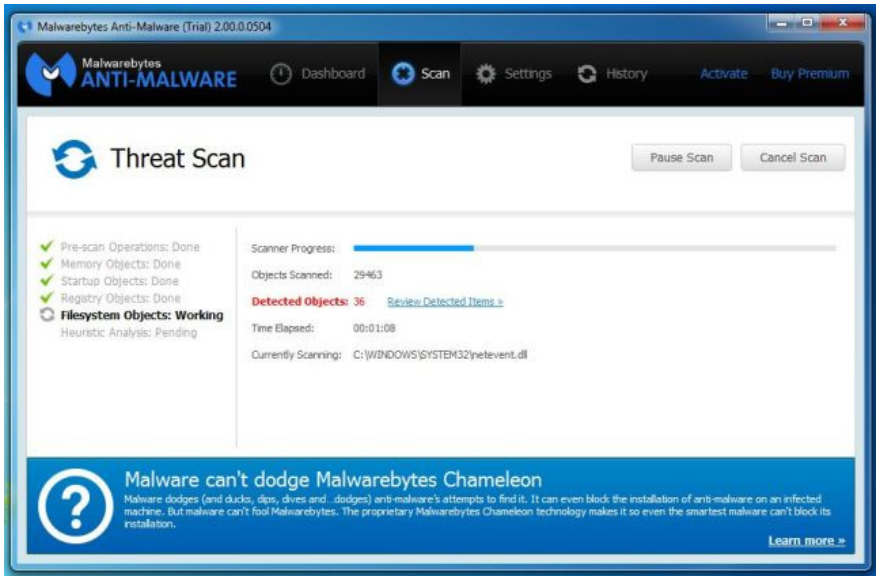
Alternatively, click the **Scan** tab, then select **Threat Scan** , then click the **Scan Now** button.



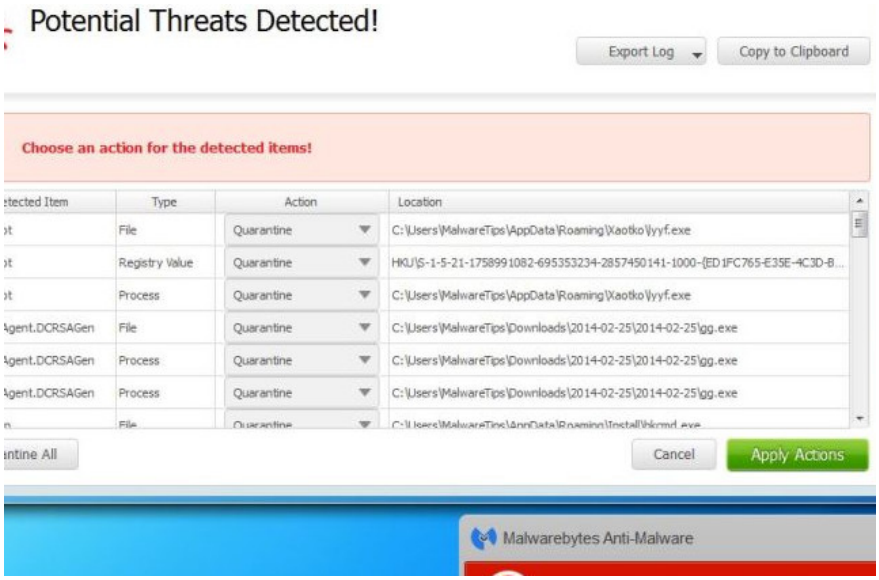
5. Malwarebytes Anti-Malware will check the update version and if any updates are available, click the **Update Now** button.



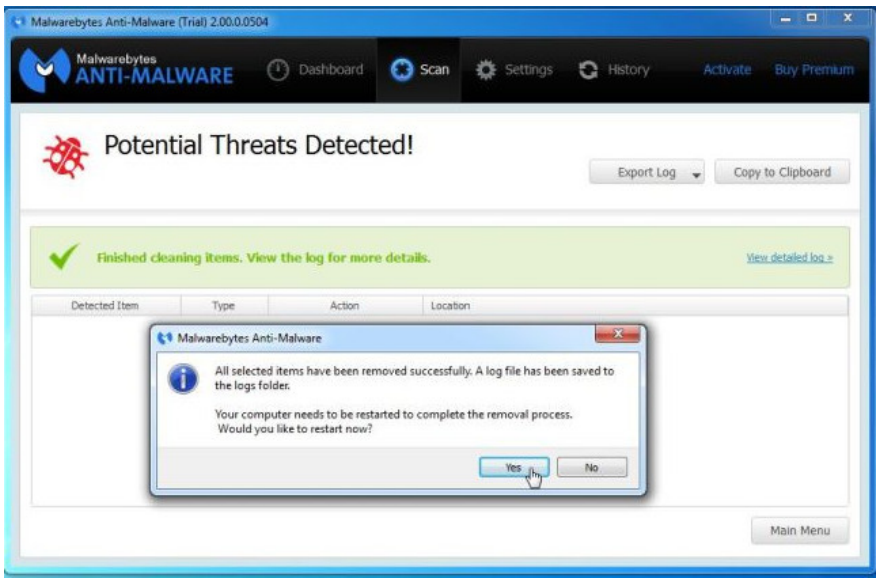
6. Malwarebytes Anti-Malware will start scanning your system to find and remove malware.



7. After the scanning process has finished, a window will appear displaying all the files and malicious programs detected by Malwarebytes Anti-Malware. To remove the malicious programs detected by Malwarebytes Anti-Malware, click the **Quarantine All** button and click the **Apply Now** button.



8. Malwarebytes Anti-Malware will remove all the malicious files, programs and registry keys it finds. During the removal of these files, Malwarebytes Anti-Malware may require a reboot of the computer to complete the process.



Step 3: Scan the system with HitmanPro

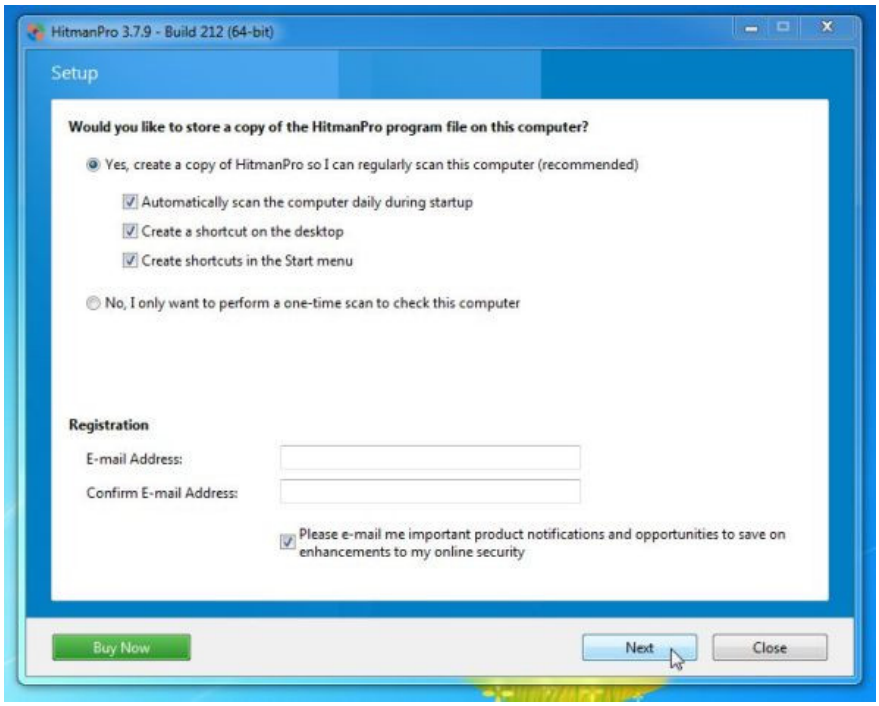
HitmanPro finds and removes malicious programs (malware), advertising programs (adware), system threats and even viruses. The program is designed to run with antivirus programs and other security tools.

1. Download HitmanPro to your device and install it.

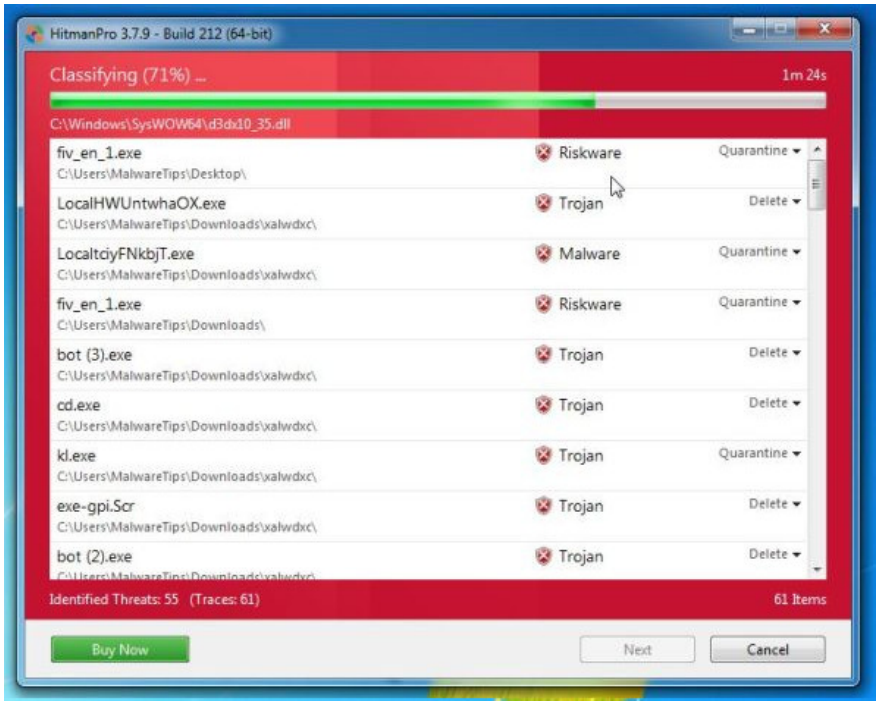
Download HitmanPro to your device and install it here.

2. Double-click the file named 'HitmanPro.exe' (if using a 32-bit version) or double-click the file 'HitmanPro_x64.exe' (if using a 64-bit version).

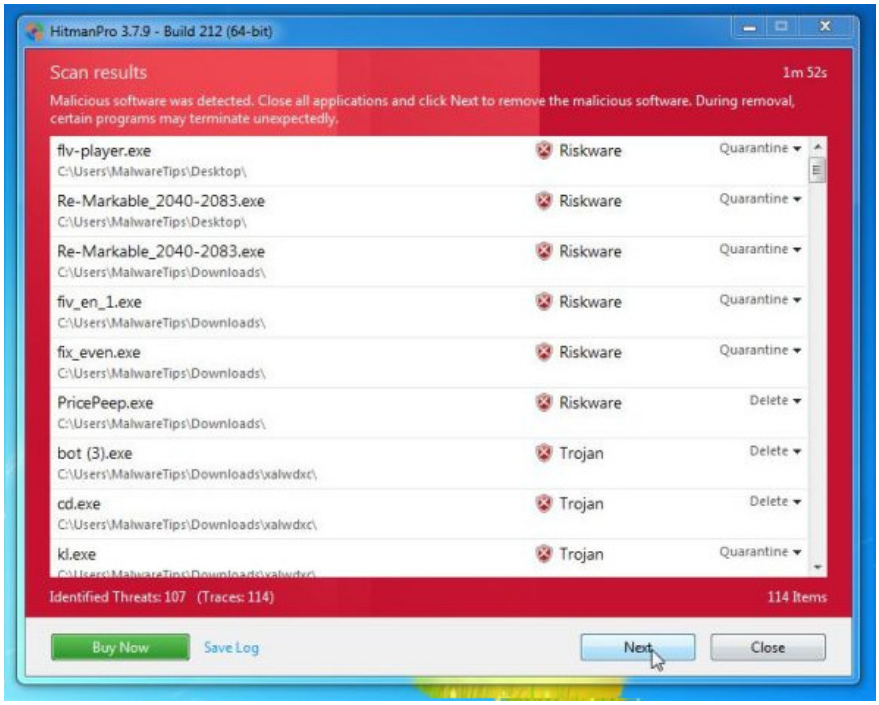
Click **Next** to install HitmanPro on your computer.



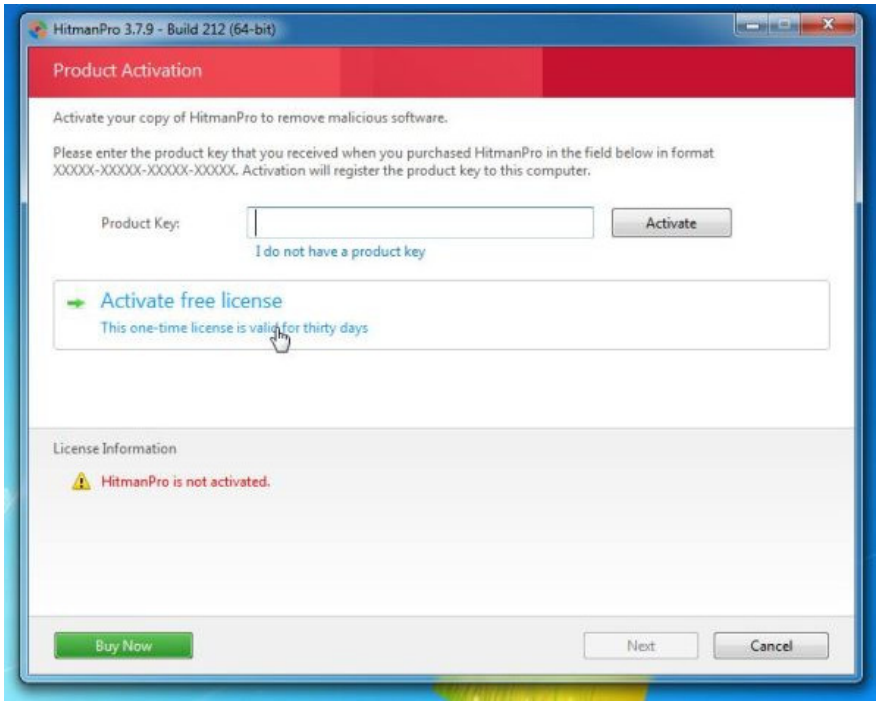
3. And HitmanPro will start the process of scanning **malicious programs** (malware) on your system.



4. After the process finishes, HitmanPro will display the list of malicious programs (malware) that it finds on your system. Click **Next** to **remove** the malicious programs.



5. Click the **Activate free license** button to try HitmanPro for 30 days and to remove the malicious files from your system.



Solution 2: Remove FBI MoneyPak virus with HitmanPro Kickstart

If you cannot start your computer in **Safe Mode with Command Prompt** , you can use **HitmanPro Kickstart** to remove **FBI MoneyPak virus** .

If the **FBI MoneyPak ransomware** attacks your computer, you will have to create a USB Bootable drive containing the HitmanPro Kickstart program. Then you use the USB Bootable drive to boot up your computer and use the program to clean up the virus and you can access your Windows computer in normal mode.

Also you need to prepare a USB drive, note that all data in the USB drive will be formatted clean, so you should use a USB drive that does not contain any important data.

1. Download HitmanPro Kickstart to your device and install.

Download HitmanPro Kickstart to your device and install it here.

2. After downloading HitmanPro Kickstart, plug in your USB drive and computer. Then double click on the file named **HitmanPro.exe** (with Windows 32-bit version) or **HitmanPro_x64.exe** (with Windows 64-bit version).

To create a HitmanPro USB Bootable drive, refer to the steps in the video below:

3. Now **remove the HitmanPro Kickstart USB drive** , plug in the **FBI MoneyPak** infected **computer** .

4. After plugging in the HitmanPro Kickstart USB drive, proceed to shut down the FBI MoneyPak virus computer, then open it again. As soon as your computer opens, look for the option saying how to access the Boot menu.

Keys related to the Boot menu are **F10, F11** or **F12** .

5. After you have identified the key (usually **the F11 key**) you need to access the Boot Menu, restart your computer again and press the boot key immediately.

Next, scan the system with HitmanPro Kickstart following the steps in the video below:

6. HitmanPro will restart your computer and Windows will boot in the normal state.

In addition, you can use other antivirus programs like Malwarebytes Anti-Malware and HitmanPro to scan the system again.

Solution 3: Use Kaspersky Rescue Disk to remove FBI MoneyPak virus

If you use the above solutions and still not "clean" the virus to attack your system, then you can use Kaspersky Rescue Disk Bootable to clean the Windows Registry and perform system scans to remove the FBI virus. MoneyPak.

To create a Bootable Kaspersky Rescue Disk drive, you need to prepare:

1. A computer that is not infected with viruses, can access the Internet.
2. A blank DVD or CD drive.
3. A computer can burn DVDs or CDs.

Step 1: Download and create Bootable Kaspersky Rescue Disk CD drive

1. Download Kaspersky Rescue Disk to your computer and install it.

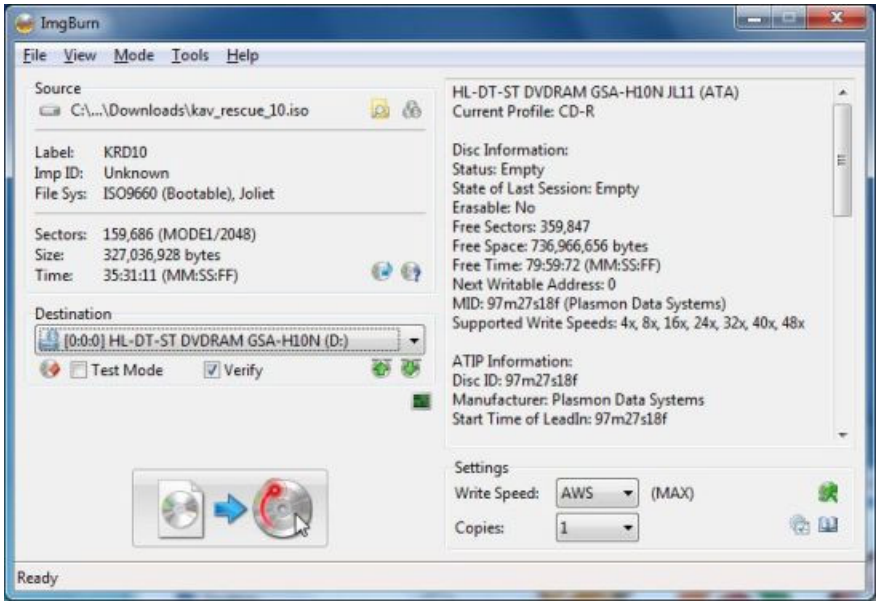
Download Kaspersky Rescue Disk to your computer and install it here.

2. To create a Bootable Rescue Disk drive, you need to use the ImgBurn program.

Download ImgBurn to your device and install it here.

3. Insert the blank CD or DVD drive, then open ImgBurn and click the **Write image file to disc button** .

4. In **Source,** click **Browse for file** button, then navigate to the previous location where you **saved Kaspersky Rescue Disk** (kav_rescue_10.iso), then click Write.

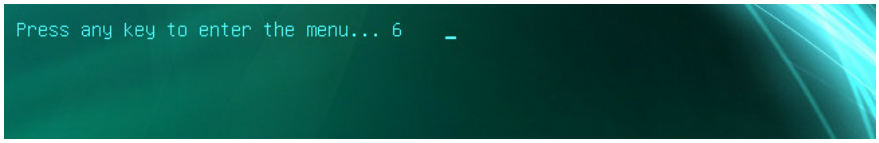


And ImgBurn will start burning your Bootable Kaspersky Rescue Disk drive.

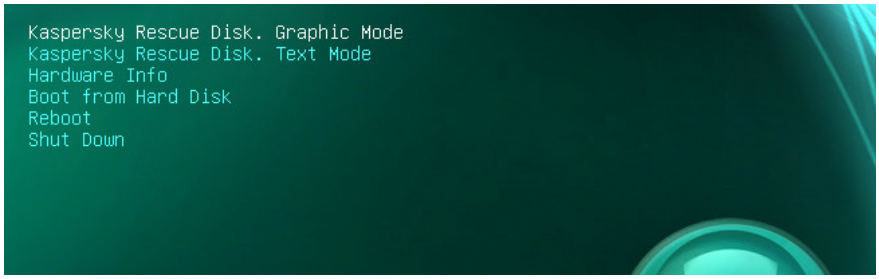
Step 2: Start your computer with Kaspersky Rescue Disk

1. After Kasperky Rescue Disk is installed, insert Kasperky Rescue Disk into the infected computer, then turn off the computer and reopen it again.

2. After your computer starts up, you will see a message prompting you to press any key to access Menu (press any key to enter the menu), press any key to start the computer. Your computer from **Kaspersky Rescue Disk** .

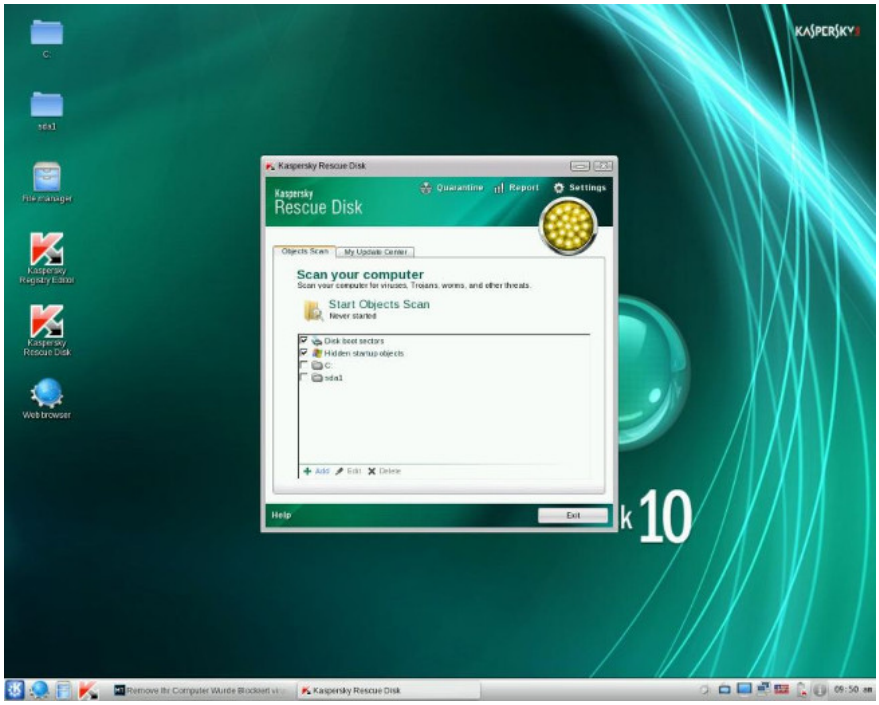


3. On the next screen, select a language, then click **Kaspersky Rescue Disk. Graphic Mode** and press **Enter** to open Kaspersky Rescue Disk.

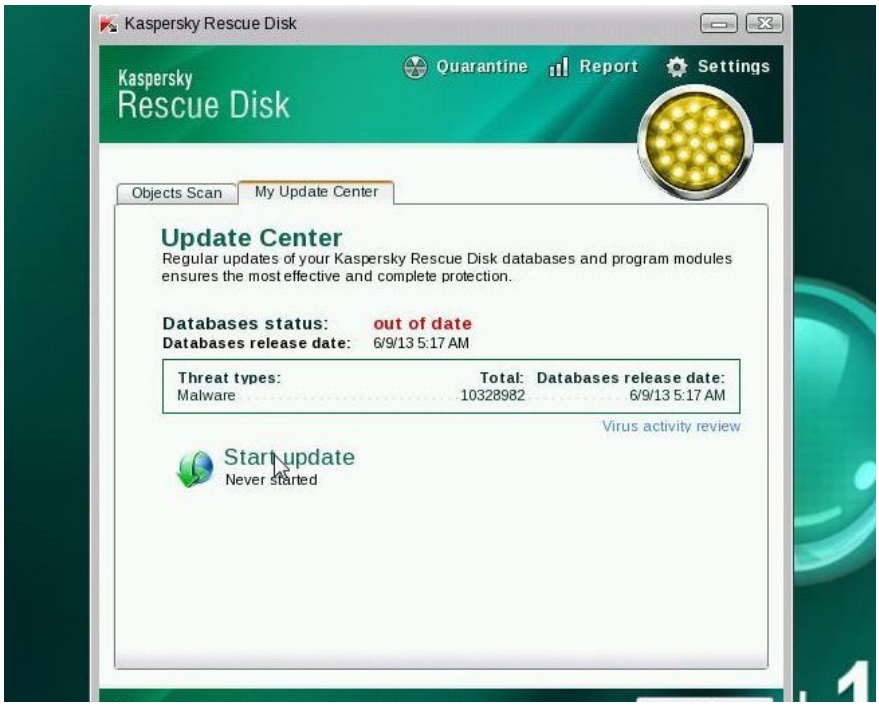


Step 3: Scan your system using Kaspersky Rescue Disk

1. A few minutes later you will see the full operating environment, and the Kaspersky Rescue Disk window will appear.

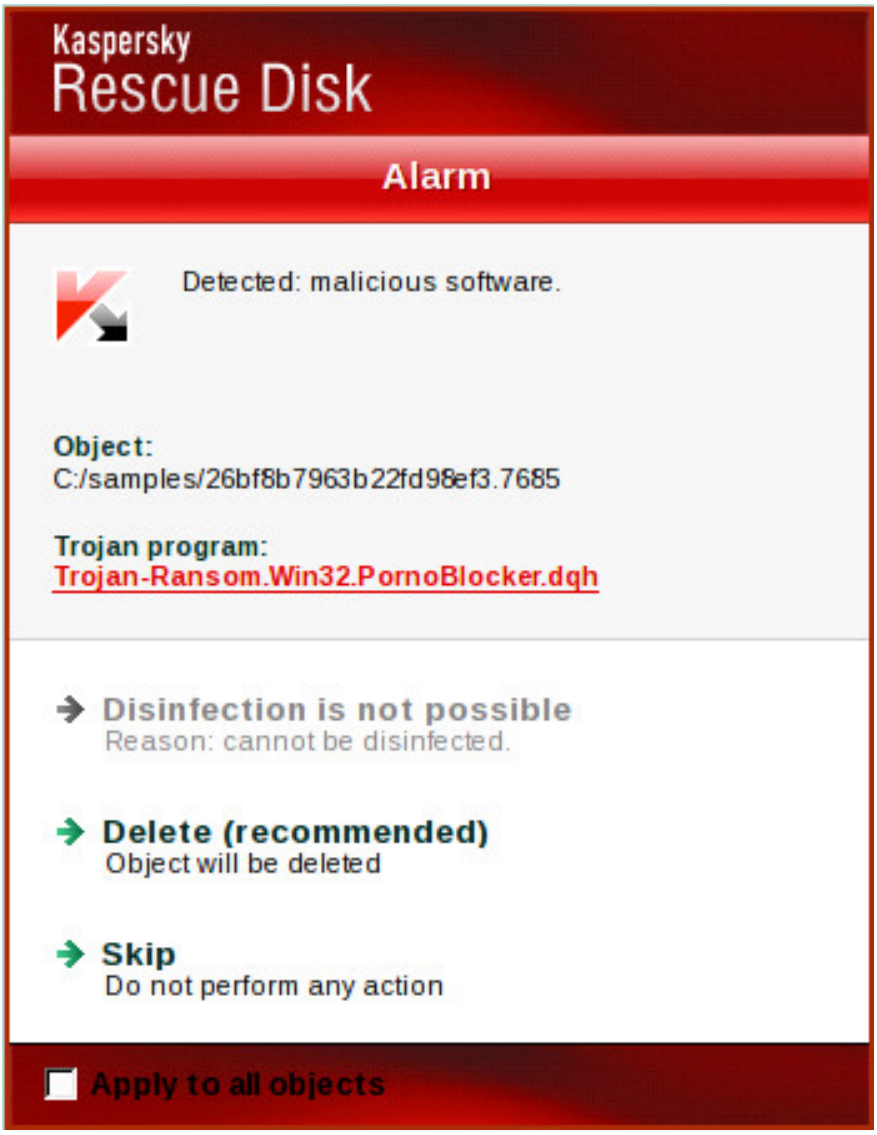


2. In the Kaspersky Rescue Disk window, go to the **My Update Center** tab, then click the **Start update** button to download the latest version of the program. Patiently waiting for the process to complete.



3. Next go to the **Objects Scan** tab, select the drive you want to scan, and then click the **Start Objects Scan** button.

4. **Kaspersky Antivirus** will find and detect FBI MoneyPak virus, you will be notified to select an action. Click on **Quarantine** or **Delete** to remove the FBI MoneyPak virus on your computer.



5. After completing the process you can boot your computer back to normal mode. To do this, click on the **Start Kaspersky** button (bottom left corner), then select **Restart** .

In addition, you can use other antivirus programs like **Malwarebytes Anti-Malware and HitmanPro** to scan the system again.

Refer to some of the following articles:

1. Rooted Delta Search on Chrome, Firefox and Explorer browsers
1. Learn from AZ about Thumbs.db, Desktop.ini and .DS_Store files
1. To remove web ads - Social 2 Search Ads, read this article

Good luck!

You finished reading the article "**What is the virus 'FBI MoneyPak' and what to do when attacked by the 'FBI MoneyPak' virus?**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.