How to remove the FBI virus (FBI Moneypak Ransomware) – Fake FBI Malware Removal Options

509 Replies
inShare34
10

What is the FBI Moneypak Virus – FBI virus?

The **FBI virus,** also referred to as the FBI Moneypak virus, Citadel Reveton, and others are terms for 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 lock computer systems (Your PC is blocked). The FBI virus applies a variety of unethical tactics, including *social engineering* in attempt to persuade unsuspecting victims to pay an unnecessary fine by making fraudulent claims that the computer has been involved in illegal activity (cyber crime) (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 you (the computer owner) may see jail time if the fine is not paid in time.

Green Dot Moneypak cards are prepaid credit cards you can purchase at Walmart or Walgreens type stores (Moneypak card).

Please note, this occurrence is the symptom of dangerous malware called ransomware. The claims made by the FBI virus on the fake FBI page are not real. **You are not in trouble with the**

FBI, paying the fine using Ukash vouchers and Moneypak cards will not fix this particular malware,and using an activation number to remove the FBI virus will likely initiate a response that leads to further complications.

If your computer is infected with the FBI virus **remove the virus immediately** using the options provided in this article.

1. **Click here to skip to FBI virus removal options (Windows PC) >>**
2. **Click here for FBI Cyber Department virus removal (Mac OS X) >>**

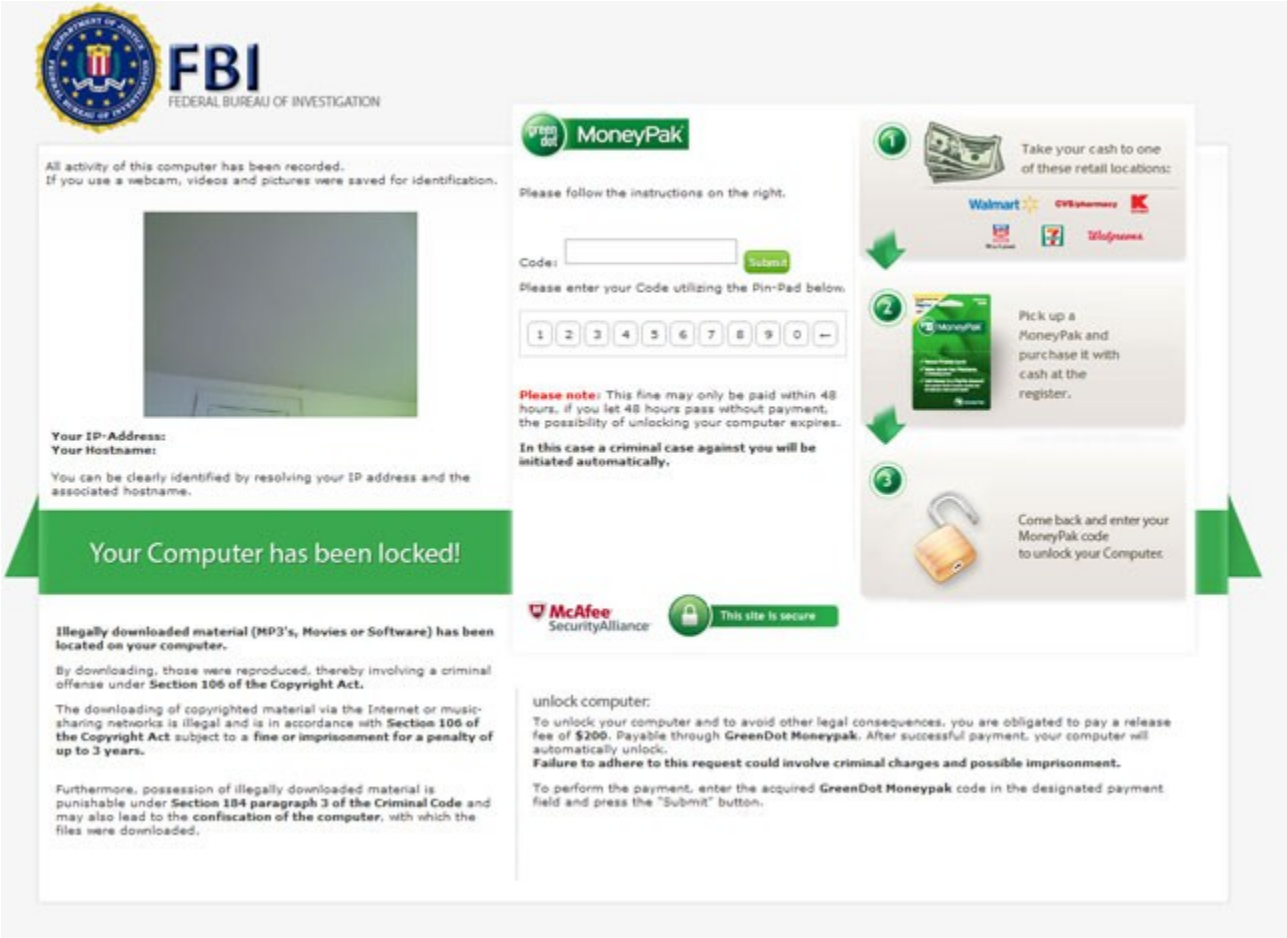
Similar Ransomware:

Department of Justice virus, United States Cyber Security Virus, Citadel Reveton, International Police, Central Police Unit, FBI DNSChanger Virus …view all

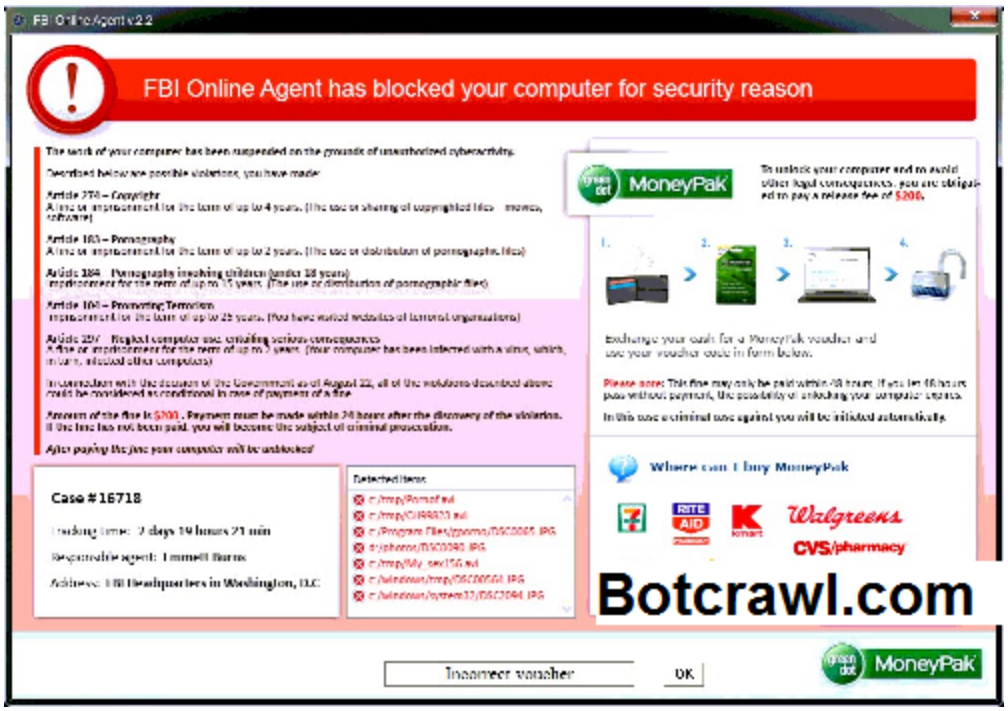
FBI virus screen shots and updates

There are several different variants of malware or FBI computer viruses that infects computer systems primarily disguised as the FBI. These different versions of the FBI cryptovirus will also display different fake FBI lock-screens. Though the FBI screens, claims, notifications, and warnings may be different, the removal steps to remove FBI viruses are essentially identical.

The first version (above) is the most popular form of the FBI virus and demands a payment of $100 while the second version (below) demands $200.



New Variant: FBI Online Agent Virus



This is the messasge displayed by the new FBI Online Agent virus:

FBI Online Agent has blocked your computer for security reason
The work of your computer has been suspended on the grounds of unauthorized cyberactivity.
Described below are possible violates, you have made:
Article 274 – Copyright
A fine or imprisonment for the term of up to 4 years. (The use or sharing of copyrighted files – movies, software)
Article 183 – Pornography
A fine or imprisonment for the term of up to 2 years. (The use or distribution of pornographic files).
Article 184 – Pornography involving children (under 18 years)
Imprisonment for the term of up to 15 years. (The use of distribution of pornographic files)
(...)

New Variant: FBI Ultimate Game Card

There is a new variant of FBI malware which uses the "Ultimate Game Card pay by cash" payment system. This new Ultimate Game Card variant of FBI ransomware does not typically hijack webcam settings.

- Click to view screenshot
- Click to view Ultimate Game Card article

New Variant: Department of Justice – FBI Black Screen of Death Virus

- Click to view screenshot
- Click to view FBI Black Screen of Death virus article

New Variant: FBI Audio Virus

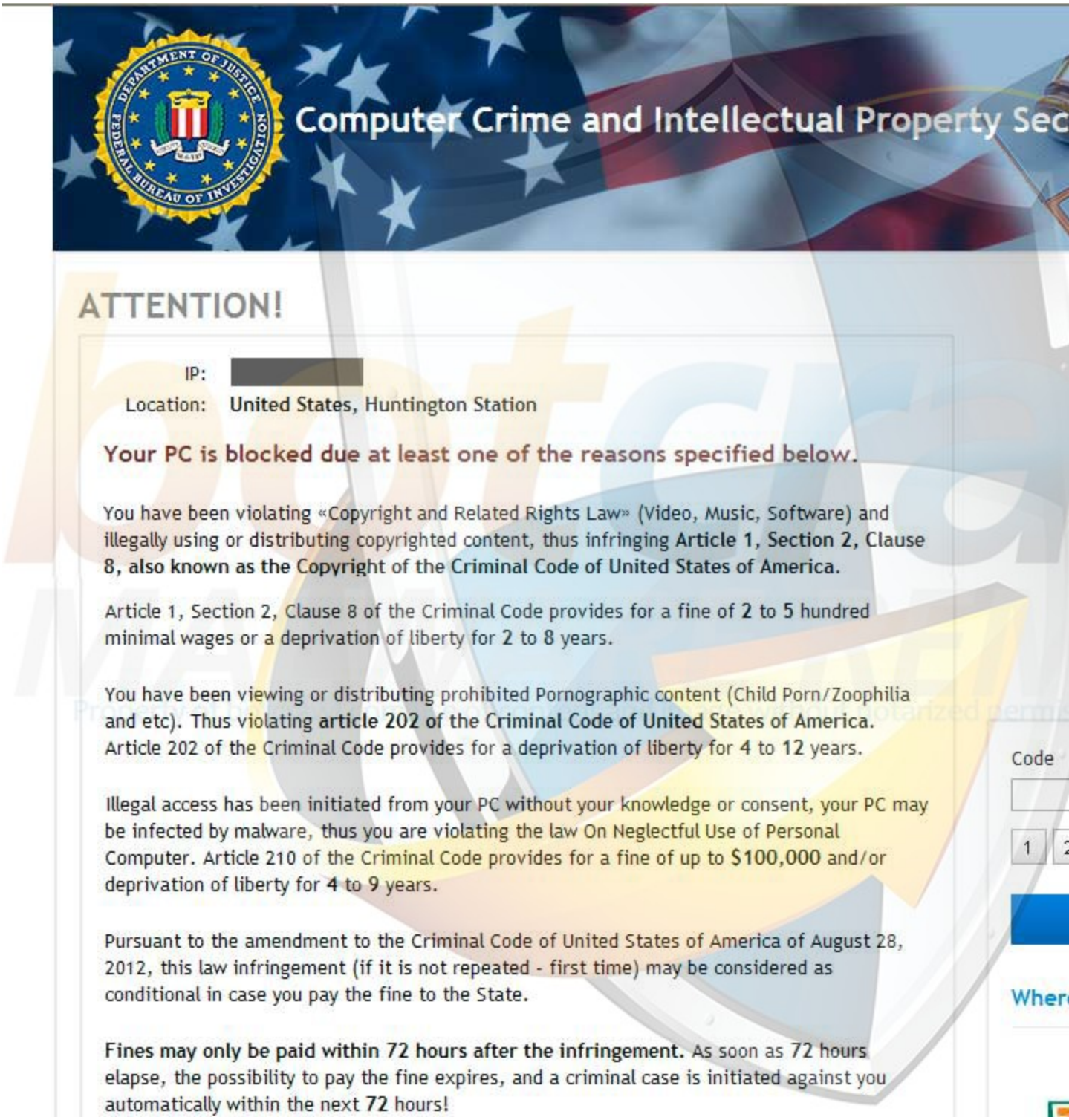
A new version of the FBI virus has been infecting computers without a FBI warning screen (black screen), only streaming audio stating the computer is locked by the FBI, etc. This version of the FBI virus is often referred to as the FBI song, the FBI audio virus, the Black screen virus, Black audio virus, FBI sound virus, and other loose references.

New Variant: FBI Cybercrime Division Virus

This new version of the FBI virus is referred to as the $300 FBI virus, FBI Cybercrime division virus, and International Cyber Security Protection Alliance virus.

- Click to view FBI Cybercrime Division article

New Variant: Computer Crime and Intellectual Property Section virus



- Click to view FComputer Crime and Intellectual Property Section article

FBI Moneypak virus: Dangers and Symptoms

Detailed below are procedures, symptoms, tactics, and dangers of the FBI virus.

- The FBI virus causes the computer system to **lock,** not allowing the user to access the computer's desktop, nor access the internet.
- Once the computer is infected the user is directed to a **fraudulent FBI screen.**
- The fraudulent FBI page/screen/website (as with most ransomware) details an alert message that reads:

"Attention! Your PC is blocked due to at least one of the reasons specified below":

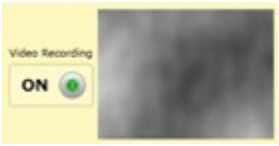
You have been violating Copyright and related rights Law (Video, Music,Software) and illegally using or distributing copyrighted content, thus infringing Article I, Section 8, clause 8, also known as the Copyright of the Criminal Code of United States of America. If it is PCEU Virus then this is thus infringing Article 128 of the criminal code of Great Britain.

The ransomware details that you have been viewing or distributing prohibited pornographic content (Child Pornography/Zoofilia). Thus violating article 202 of the Criminal Code of United States of America. Article 202 of the criminal provides for deprivation of liberty for two or twelve yours.

Illegal access to computer data has been initiated from your PC,or you have been. Article 210 (it is 208 for PCEU Virus) of the Criminal Code provides for a ***fine of up to $100,000*** *and/or a deprivation of liberty for four to nine years.*

Fines may only be paid within 72 hours after the infringement. As soon as 72 hours elapse, the possibility to pay the fine expires, and a criminal case is initiated against you authomatically within the next 72 hours! (Sometimes it shows you within 2 hours or 48 hours).

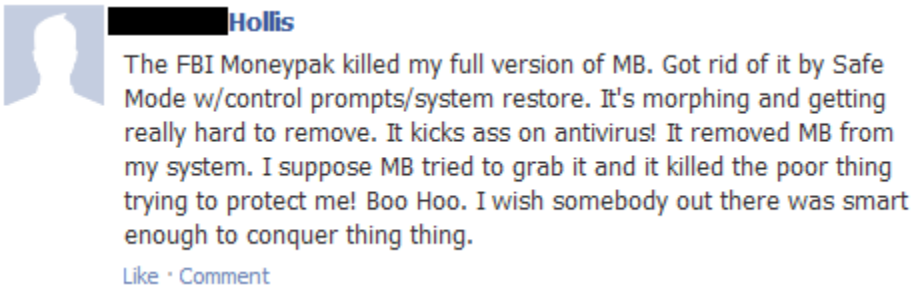
Web cam control



The FBI virus and ransomware alike often control the web cameras (webcam, web cam) of computer systems they infect. When the computer user is taken to the fake FBI drive-by-download website (or the screen simply pops up), a streaming video is displayed from the users connected webcam. The ransomware virus screen or page may display the webcam as "recording". If you do not have a web cam connected the video screen will appear blank and will still show as recording. The FBI virus and alike malware are capable of recording your through your webcam and connected audio interfaces, such as microphones and audio production equipment.

Antivirus/Anti-Malware Software malfunction/termination

The FBI Moneypak virus may cause Antivirus software to malfunction. Anti Malware and Antivirus programs can be used to scan and remove the FBI Moneypak virus but in many scenarios the infection has progressed far enough to disable removal software. There are steps around this, such as entering your system in safe mode or restoring your computer, unplugging from the internet, denying flash, using the optical disk drive option, safe mode with networking, or slaving your HDD.



This Facebook user removed FBI Moneypak malware by entering Windows in "Safe Mode With Command Prompt" and performing a restore. Instructions to perform system restores using safe mode are outlined further below.

Telephone Phishing: Fake phone calls

In some reported instances, victims have received phone calls from criminals claiming to be Microsoft employees (etc.) informing them that their computer systems has been infected with malware, etc. These phone calls are in relation to this particular crypto-virus (read more here). If you receive any calls like this, keep in mind these are not Microsoft employees (nor a realistic service), and contact the proper law enforcement depending on your geographic location (you may report criminal activity here). These phone calls are defined as "phishing" schemes and may or may not be related to the FBI Moneypak virus.

What happens if the FBI virus is not removed?

If you are infected with ransomware such as the FBI virus, your personal and private data and computer system functionality is already at a very high risk. If the infected computer is powered ON and connected to the internet, Trojans horses may have complete control of the computer system and access to every piece of stored data.
The main purpose of this ransomware is to target and scare unsuspecting victims into believing they are in trouble with a department of authority in order to willingly pay the fine stated on the prompted "alert page", but that does not mean the infection will not hibernate (remain undetected) on an infected system in order to exploit vulnerabilities utilizing other malicious practices aside from locking the system. It has been reported that the FBI virus *may collect private information while remaining in the background.*

How to remove the FBI Moneypak Ransomware Virus (FBI Viruses)

Different victims of the FBI Moneypak virus will require separate removal steps due to the progress of the infection. Some users can not access the internet, nor their desktops and some still can. Since this is the case, we have outlined easy options to remove FBI Moneypak for all victims.

FBI Virus Removal Options (Ransomware)

1. **Malware Removal Software** – Scan and remove malware
2. **Manual Removal (Advanced)** – Remove associated files
3. **System Restore (Windows)** **Refresh/Reset (Windows 8)** – Restore PC to a date and time before infection (includes different access options)
4. **Safe Mode With Networking** – Manually remove files and/or scan and remove malware (reset proxy settings if needed)
5. **Flash Drive Option** – Load Antivirus (AM) software to a flash drive, scan and remove malware
6. **Optical CD-R Option** – Scan and remove malware
7. **Slave Hard Disk Drive Option** – Scan, detect, and remove malware

Please click a removal option above to automatically scroll to the instruction below.

Removal Tips

The safest option to remove the FBI Moneypak 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 Moneypak 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 Moneypak 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 the 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 Window's 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 Moneypak virus utilizes flash and in some cases, disabling (denying) flash can "freeze" the FBI Moneypak 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 (detailed below): 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.

1. Malware Removal Software

Use these directions to automatically remove the FBI virus using Malwarebytes Anti-Malware software. Additional FBI virus removal software and tools are detailed below, including AVG and Symantec Norton.

1. Install the free or paid version of **Malwarebytes Anti-Malware**

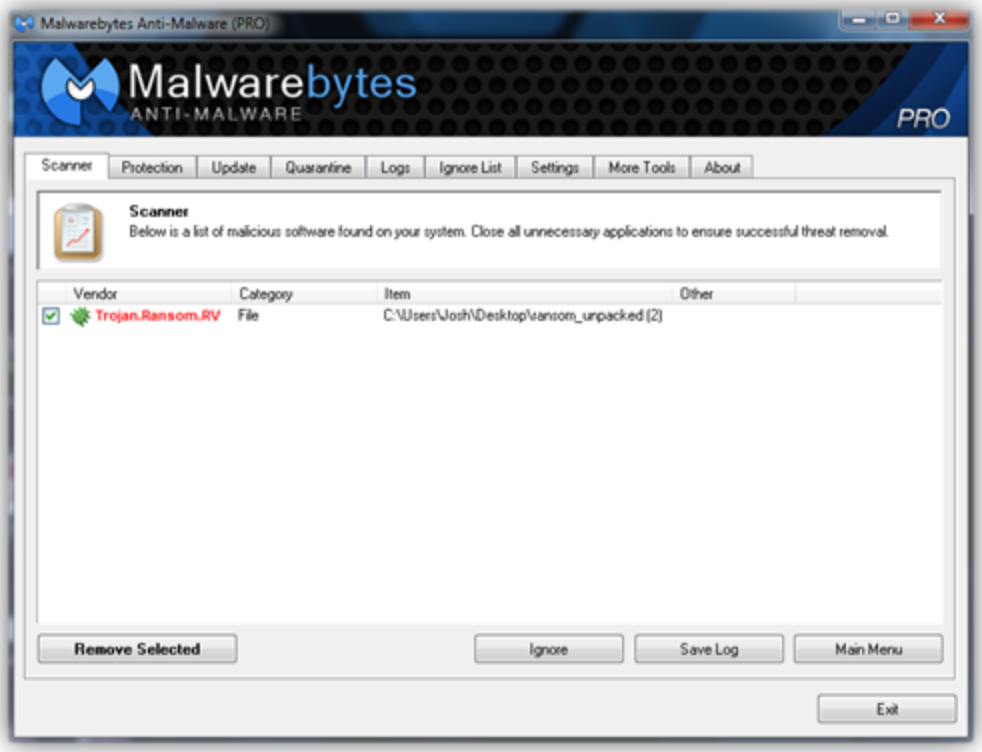
Malwarebytes Anti-Malware **Editor's Choice**

$24.95 USD (Lifetime) / FREE

Latest versions: Malwarebytes Anti-Malware PRO, Malwarebytes Anti-Malware Free (1.70.0.1100)
Release date: 2013

2. *Open* Malwarebytes and run a Full System Scan by selecting the **Perform full scan** radio option followed by clicking the **Scan** button (pictured below).

3. Malwarebytes will automatically detect malware on the computer system and once the scan is complete Malwarebytes will display the malicious results. Make sure to finish the scan by selecting the malicious file and clicking the **Remove Selected** button.



Additional Removal Software

The software listed below are strongly suggested to remove ransomware and further protect against related intrusions.

SurfRight

$24.95 USD (1 Year) / FREE

Latest version: HitmanPro 3
Release date: 2013 / 3.7

Purchase Free Download

Norton by Symantec Editor's Choice

$79.99 USD (1 Year)

Latest version: Norton 360™ 5.0
Release date: 2013

Purchase All Products

AVG Antivirus Editor's Choice

$39.99 USD (1 Year) / FREE

Latest versions: AVG Antivirus 2013, AVG Free Antivirus
Release date: 2013

Purchase Free Download

Avira Antivirus

$36.99 USD (1 Year) / FREE

Latest versions: Premium 2013, Avira Free Antivirus
Release date: 2013

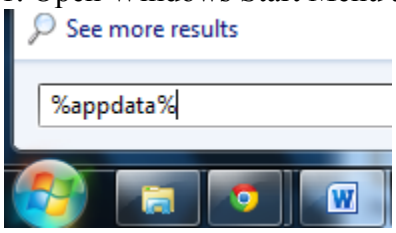
Other: Microsoft Defender (free), Microsoft Security Essentials (free)

2. Manual Removal (Advanced)

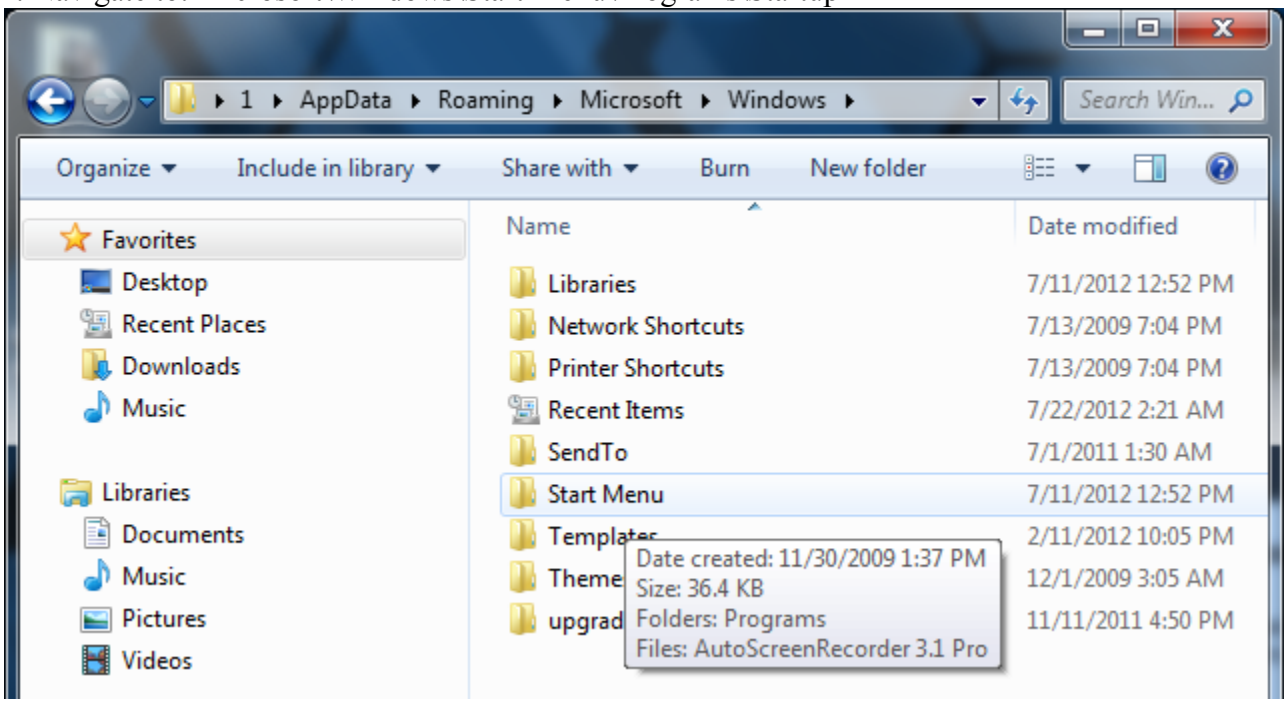
If this option does not help you locate the malicious files, skip it. Do not be alarmed if some files described below are not found in your particular infection, such as the *ctfmon* file.

We are going to enter your computers App Data (Application Data), which is a hidden folder with hidden files. To learn how to show hidden files click here.

1. Open Windows Start Menu and type **%appdata%** into the search field and press Enter.

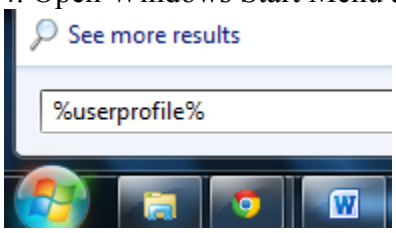


2. Navigate to: Microsoft\Windows\Start Menu\Programs\Startup

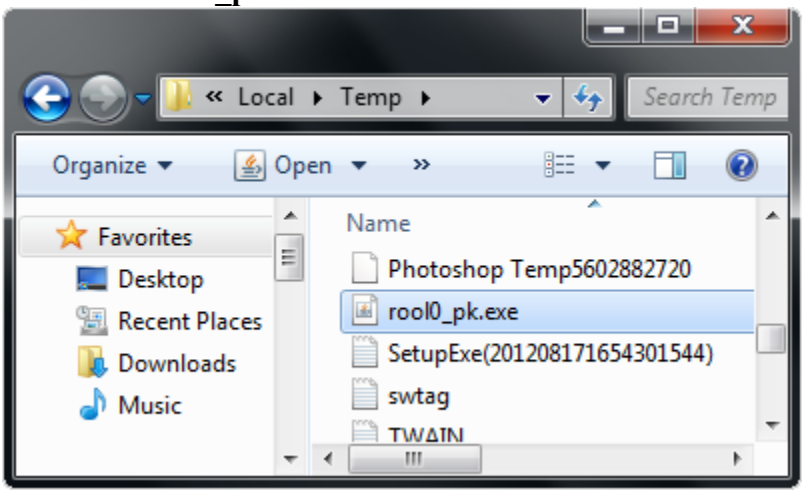


3. Remove **ctfmon** (ctfmon.lnk if in dos) – this is what's calling the virus on start up. This is not ctfmon.exe.

4. Open Windows Start Menu and type **%userprofile%** into the search field and press enter.



5. Navigate to: Appdata\Local\Temp
6. Remove **rool0_pk.exe**



7.Remove **[random].mof** file
8. Remove **V.class**

The virus files may have names other than "rool0_pk.exe" but file names should appear similar with the same style of markup. There may also be 2 files, 1 being a *.mof* file. Removing the *.exe* file will fix FBI Moneypak. The class file uses a java vulnerability to install the virus and removal of *V.class* is done for safe measure.

All FBI Moneypak Files:

The files listed below are a collection of what causes FBI Moneypak to function. To ensure FBI Moneypak is completely removed via manually, delete all given files if located. Keep in mind, [random] can be any sequence of numbers or letters and some files may not be found in your infection.

```
%Program Files%\FBI Moneypak Virus
%Appdata%\skype.dat
%Appdata%\skype.ini
%AppData%\Protector-[rnd].exe
%AppData%\Inspector-[rnd].exe
%AppData%\vsdsrv32.exe
%AppData%\result.db
%AppData%\jork_0_typ_col.exe
%appdata%\[random].exe
%Windows%\system32\[random].exe
%Documents and Settings%\[UserName]\Application Data\[random].exe
%Documents and Settings%\[UserName]\Desktop\[random].lnk
```

```
%Documents and Settings%\All Users\Application Data\FBI Moneypak Virus
%CommonStartMenu%\Programs\FBI Moneypak Virus.lnk
%Temp%\0_0u_l.exe
%Temp%\[RANDOM].exe
%StartupFolder%\wpbt0.dll
%StartupFolder%\ctfmon.lnk
%StartupFolder%\ch810.exe
%UserProfile%\Desktop\FBI Moneypak Virus.lnk
WARNING.txt
V.class
cconf.txt.enc
tpl_0_c.exe
irb700.exe
dtresfflsceez.exe
tpl_0_c.exe
ch810.exe
0_0u_l.exe
[random].exe
```

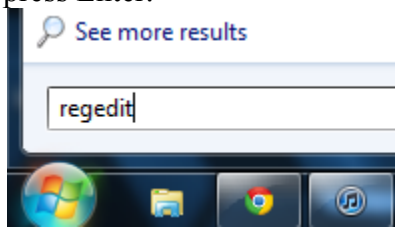
Kill ROGUE_NAME Processes:

Access Windows Task Manager (Ctrl+Alt+Delete) and kill the rogue FBI Moneypak process. Please note the infection will have a random name for the process [random] which may contain a sequence of numbers and letters (ie: USYHEY347H372.exe).

```
[random].exe
```

Remove Registry Values

To access Window's Registry Editor type **regedit** into the Windows Start Menu text field and press Enter.




```
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\[random].exe
HKEY_LOCAL_MACHINE\SOFTWARE\FBI Moneypak Virus
HKEY_CURRENT_USER \Software\Microsoft\Windows\CurrentVersion\Policies\System
'DisableRegistryTools' = 0
HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system
'EnableLUA' = 0
HKEY_CURRENT_USER \Software\Microsoft\Windows\CurrentVersion\Internet
Settings 'WarnOnHTTPSToHTTPRedirect' = 0
HKEY_CURRENT_USER \Software\Microsoft\Windows\CurrentVersion\Policies\System
'DisableRegedit'= 0
HKEY_CURRENT_USER\Software\FBI Moneypak Virus
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run 'Inspector'
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\FBI
Moneypak Virus
```

```
HKEY_CURRENT_USER \Software\Microsoft\Windows\CurrentVersion\Policies\System
'DisableTaskMgr' = 0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
Execution Options\protector.exe
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Inspector
%AppData%\Protector-[rnd].exe
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\WarnOnHTTPSToHTTPRedirect 0
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Settings\ID 4
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Settings\UID
[rnd]
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Settings\net
[date of installation]
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system\
ConsentPromptBehaviorAdmin 0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system\
ConsentPromptBehaviorUser 0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system\
EnableLUA 0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
Execution Options\AAWTray.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
Execution Options\AAWTray.exe\Debugger svchost.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
Execution Options\AVCare.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
Execution Options\AVCare.exe\Debugger svchost.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
Execution Options\AVENGINE.EXE
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
Execution Options\AVENGINE.EXE\Debugger svchost.exe
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
"DisableRegistryTools" = 0
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
"DisableTaskMgr" = 0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system
"ConsentPromptBehaviorAdmin" = 0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system
"ConsentPromptBehaviorUser" = 0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system
"EnableLUA" = 0
```

3. Restore – Recover Computer

Below we detail 3 different instructions to restore or recover a common Window's computer.

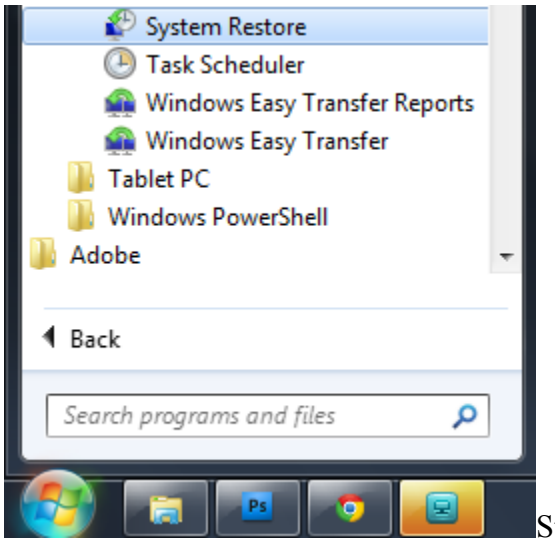
- To learn more about Windows System Restore for Vista, XP, and 7 please click here.
- For Windows 8 refresh/reset instructions please click here.

Please also keep in mind if you have the manufacture's boot disc that came with your computer, you will be able to perform a system restore or total system recovery by inserting the disc, tapping f8 (or your manufacture hotkey), and following the on screen instructions.

Windows Start Menu Rstrui.exe Restore

1. Access Windows **Start menu**
2. Type **rstrui.exe** into the search field and press **Enter**
3. Follow instructions in Window's Restore Wizard

Start Menu Restore



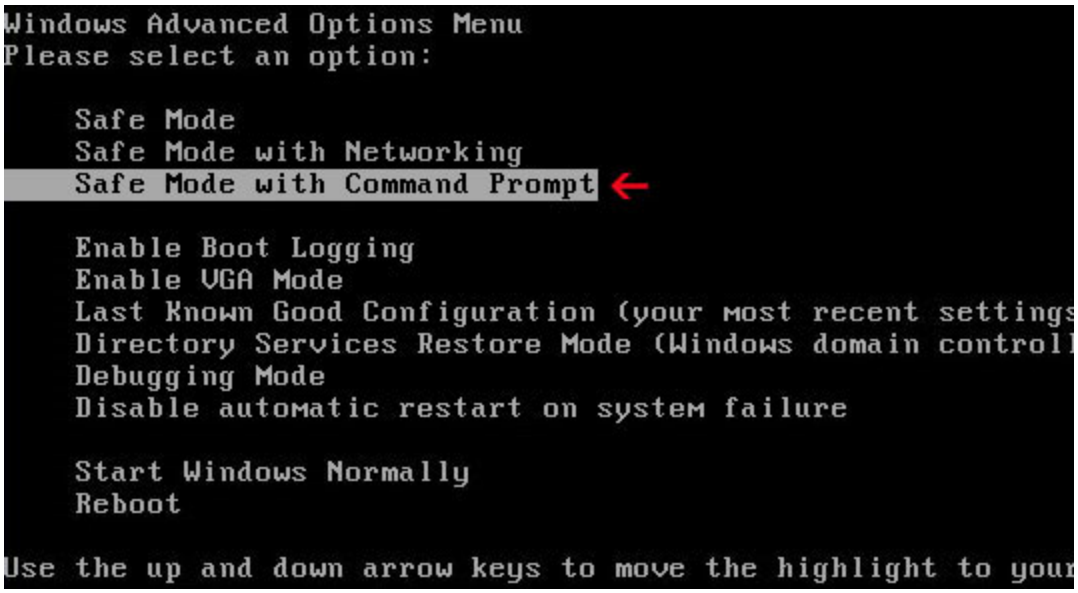
Standard directions to quickly access Window's System Restore Wizard.

1. Access Windows **Start menu** and click **All Programs.**
2. Click and open **Accessories,** click **System Tools,** and then click **System Restore.**
If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
3. Follow the simple instructions to Restore your computer to a date and time before infection.

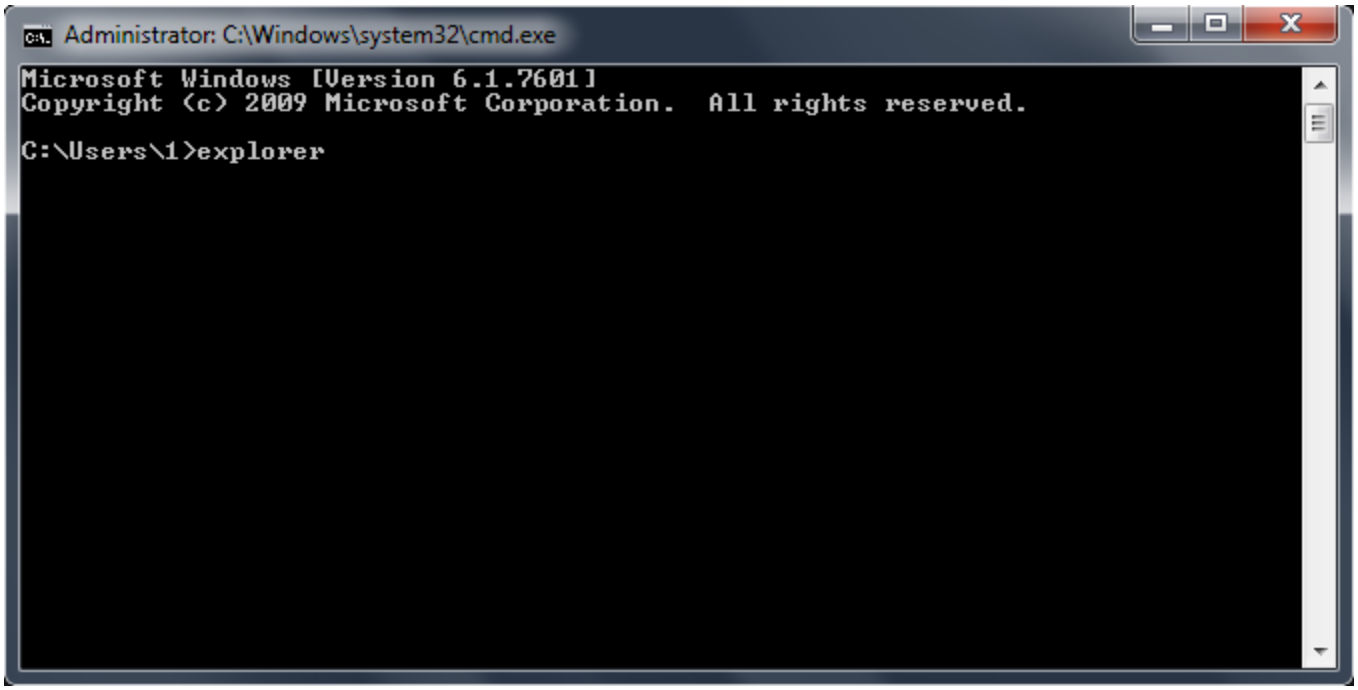
Safe Mode With Command Prompt Restore

If you can not access Window's desktop, this is the suggested step. If it is difficult to start windows in safe mode; if Windows's brings up a black screen, with "safe mode" in the four corners – Move your cursor to the lower left corner, where the Search box is usually visible in Windows Start Menu and it will come up, including the "Run" box.

1. **Restart/reboot** your computer system. Unplug if necessary.
2. Enter your computer in **"safe mode with command prompt"**. To properly enter safe mode, repeatedly press **F8** upon the opening of the boot menu.

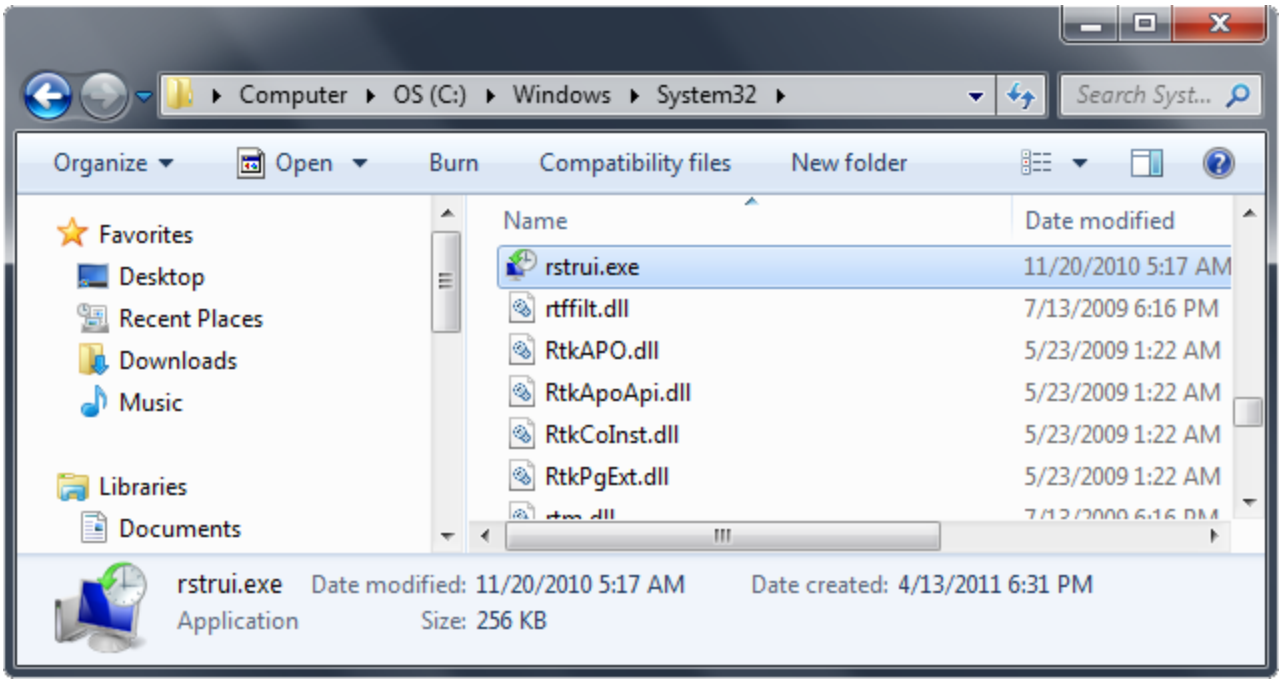


3. Once the Command Prompt appears you only have few seconds to type **"explorer"** and **hit Enter.** If you fail to do so within 2-3 seconds, the FBI MoneyPak ransomware virus will not allow you to type anymore.

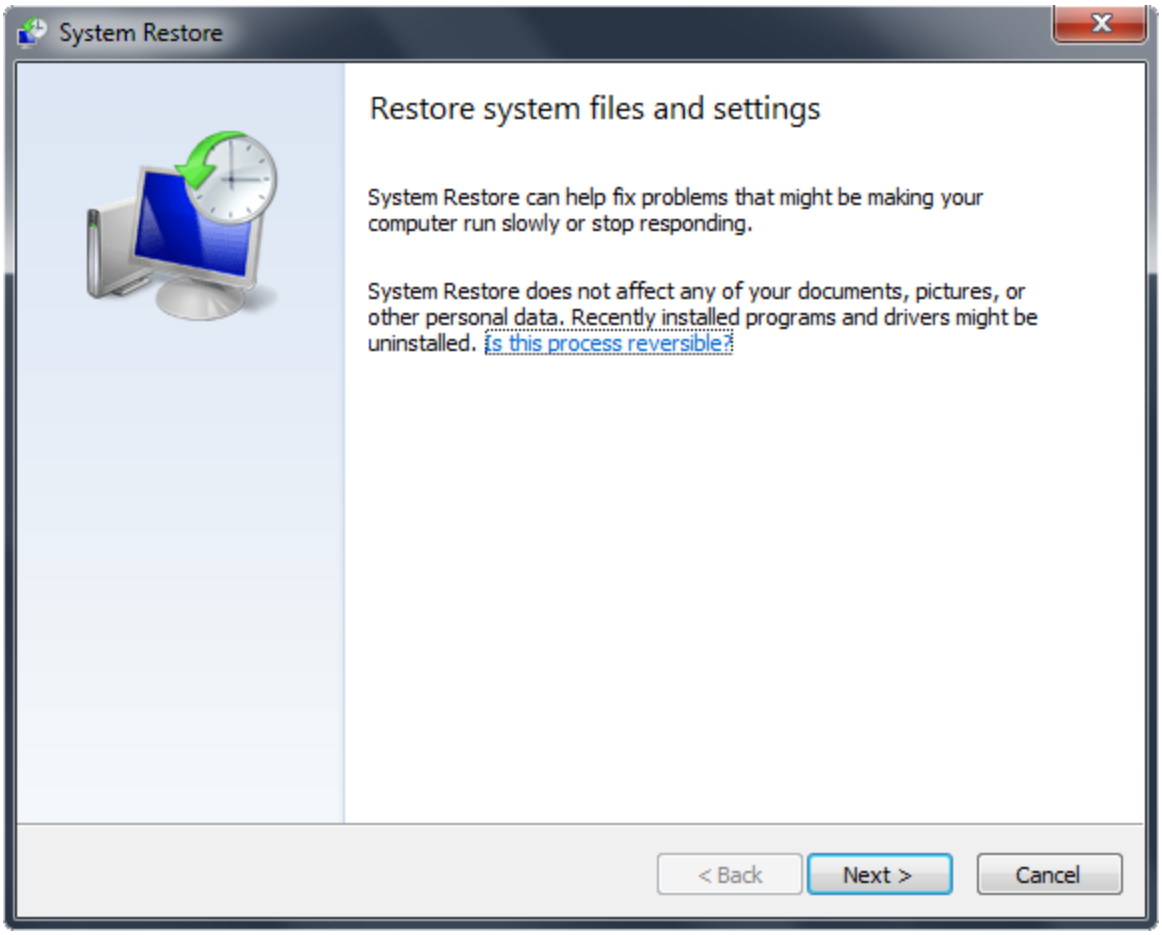


4. Once Windows Explorer shows up browse to:

- *Win XP:* **C:\windows\system32\restore\rstrui.exe** and press Enter
- *Win Vista/Seven:* **C:\windows\system32\rstrui.exe** and press Enter



5. Follow all steps to restore or recover your computer system to an earlier time and date (restore point), before infection.



More System Restore Links:

- http://botcrawl.com/how-to-restore-microsoft-windows-vista-microsoft-windows-xp-and-microsoft-windows-7/
- http://windows.microsoft.com/en-US/windows-vista/System-Restore-frequently-asked-questions

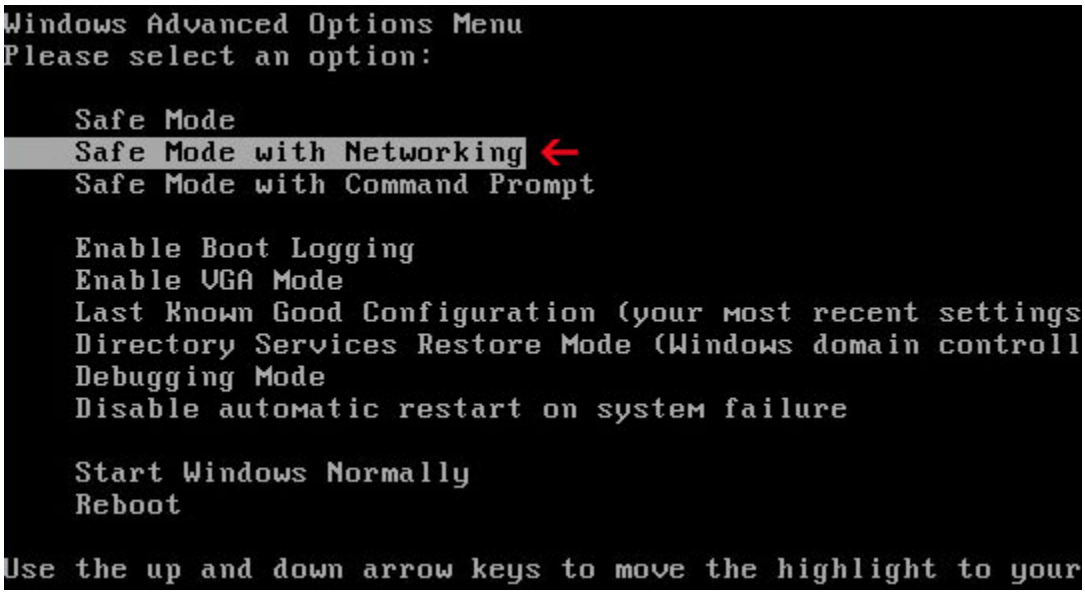
4. Safe Mode With Networking

For users needing access to the Internet or the network they're connected to. This mode is helpful for when you need to be in Safe Mode to troubleshoot but also need access to the Internet for updates, drivers, removal software, or other files to help troubleshoot your issue.

- This mode will also bypass any issues where Antivirus or Anti Malare applications have been affected/malfunctioning because of the FBI Moneypak infection's progression.

The plan with this option is to enter your computer in "safe mode with network" and install anti-malware software. Proceed to scan, and remove malicious files.

1. Reboot your computer in “Safe Mode with Networking”. As the computer is booting (when it reaches the manufacture’s logo) tap and hold the “F8 key” continuously to reach the correct menu. On the Advanced Boot Options screen, use your keyboard to navigate to “Safe Mode with Networking” and press Enter. Shown below.



- Make sure to log into an account with administrator rights.

The screen may appear black with the words “safe mode” in all four corners. Click your mouse where windows start menu is to bring up necessary browsing.

2. There are a few different things you can do…

- Pull-up the **Start menu,** enter **All Programs** and access the **StartUp** folder.
- Remove **“ctfmon”** link (or similar).

This seems to be an easy step in removing the FBI virus for many users. If you are interested in learning about ctfmon.exe please click here.

Now, move on to the next steps (which is not a necessity if you removed the file above but provides separate options for troubleshooting).

3. If you still can't access the Internet after restarting in safe mode, try resetting your Internet Explorer proxy settings. These 2 separate options and following steps will reset the proxy settings in the Windows registry so that you can access the Internet again.

How To Reset Internet Explorer Proxy Settings

- ***Option 1***

In Windows 7 click the Start button. In the search box type **run** and in the list of results click Run.

In Windows Vista click the Start button and then click Run.

In Windows XP click Start and then click Run.

Copy and paste or type the following text in the Open box in the Run dialog box and click OK:

```
reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings" /v
ProxyEnable /t REG_DWORD /d 0 /f
```

In Windows 7 click the Start button. In the search box type **run** and in the list of results click Run.

In Windows Vista click the Start button and then click Run.

In Windows XP click Start and then click Run.

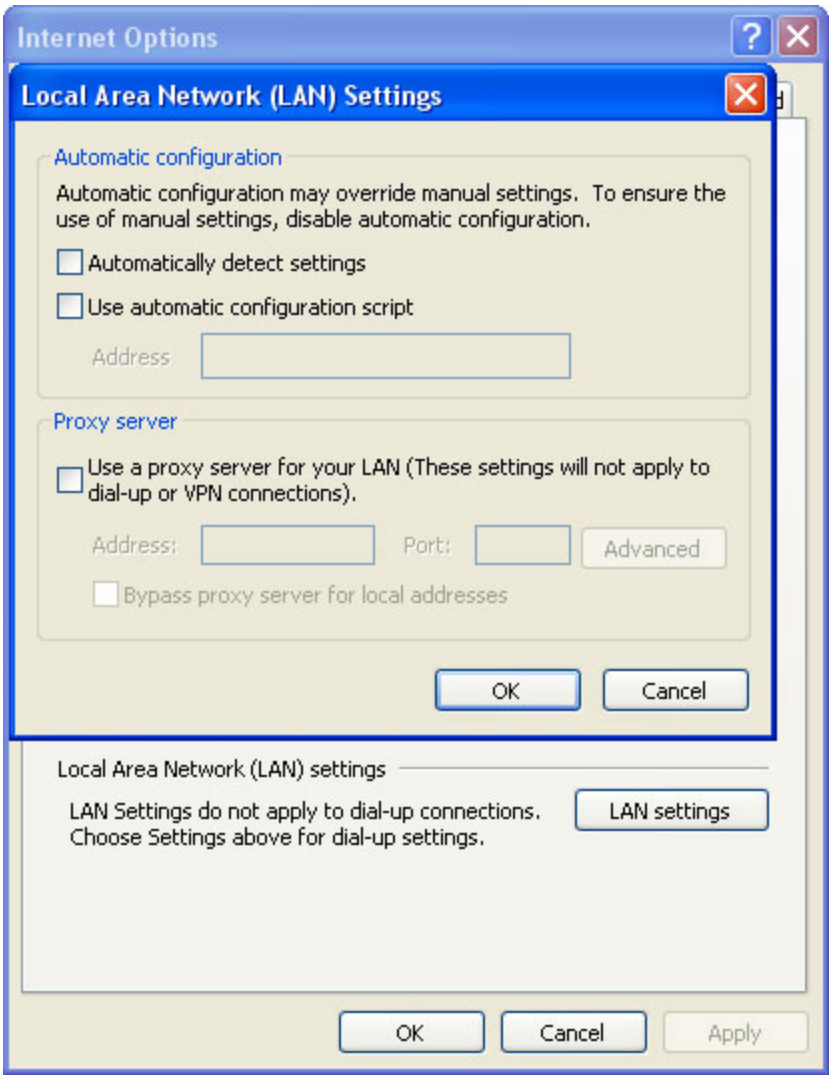
Copy and paste or type the following text in the Open box in the Run dialog box and click OK:

```
reg delete "HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings"
/v ProxyServer /f
```

Restart Internet Explorer and then follow the steps listed previously to run the scanner

- ***Option 2***

Launch Internet Explorer. In Internet Explorer go to: Tools->Internet Options->Connections tab. Click Lan Settings button and uncheck the checkbox labeled Use a proxy server for your LAN. Click OK.



4. It is now recommended to download Malwarebytes (free or paid version) and run a full system scan to remove FBI Moneypak malware from your computer if you do not have this application on your system.

5. Flash Drive Option

1. Turn off your computer system and Unplug your internet connection
2. Turn the machine back on (In some cases the virus can only open if your machine is plugged into the internet)
3. On another (clean) computer, download Malwarebytes or your preferred removal program and load the Mbam-Setup.exe (or similar) file onto the flash drive
4. Remove the flash drive from the clean computer and insert it into the affected machine, proceed to install Malwarebytes (etc) using the setup file located on the flash drive.
5. Run a full system scan, Malwarebytes will find and eradicate malicious files
6. Restart your machine

6. Optical CD-R Option

1. Place a blank CD-R into your CDROM drive
2. Download and place Microsoft Defender or your prefered removal program onto the blank CD-R
3. Restart your computer and boot from CD

“You may need an old school keyboard (not the USB, but the PC connector type) since the virus delays the USB startup. The Defender will clean your PC in totality. This virus is somehow complex, but is no match for Windows Defender. After the scan is complete, run again a full scan without a restart.”

7. Slave Hard Disk Drive Option

If you are having complications with Anti-Malware software a suggestion would be to slave your HDD, then proceed to scan. You will need a second operating computer and tools to remove your hard drive. *Please note this may be difficult for some users and there are other options to scan your hard drive during complications. This is a common practice for local computer technicians.

1. Remove the Hard Disk Drive from your computer.
2. On the circuit board side of your HDD set the drive to “slave”.
3. Connect the slave drive to an unaffected computer.
4. Scan the slave drive, and proceed to remove any malware on the drive. Make sure to scan each user account.
5. Reconnect the HDD to your original computer.