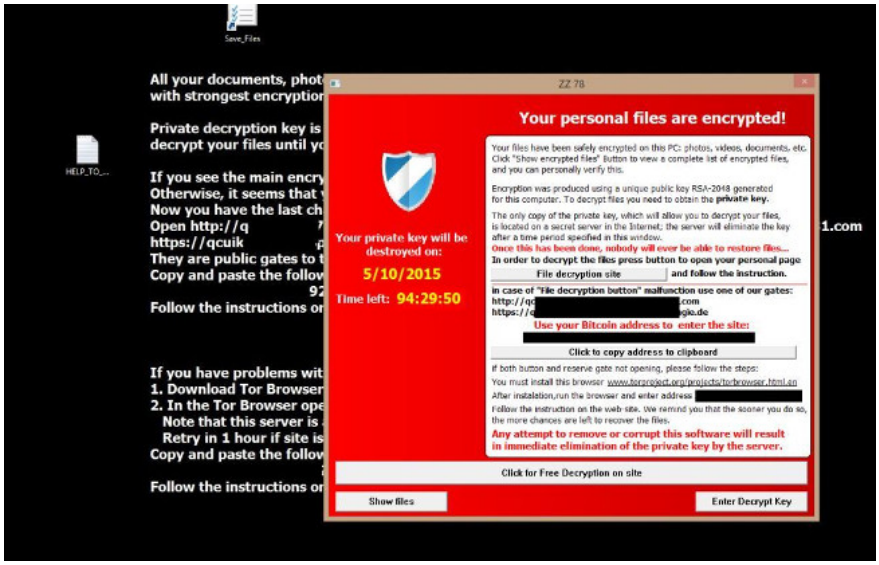
What is the 'Your personal files are encrypted' virus? How to remove it?

Ransomware Your personal files are encrypted is a program, spyware targeted at all Windows versions, including Windows 10, Windows Vista, Windows 8 and Windows 7. It is distributed through: the malicious websites or hacked websites, and it can access your computer by exploiting an exploit kits that use vulnerabilities on your computer to install the Trojan. unaware.

Ransomware " *Your personal files are encrypted* " is a program, spyware targeted at all Windows versions, including Windows 10, Windows Vista, Windows 8 and Windows 7. It is distributed through : malicious websites or hacked websites, and it can access your computer by exploiting **an** exploit kits using holes on your computer to install the Trojan but you don't know it.

Some versions of ransomware " *Your personal files are encrypted* " such as: CryptoLocker, Crypt0l0cker, Alpha Crypt, TeslaCrypt, CoinVault, Bit Crypt, CTB-Locker orTorrentLocker.



1. How does Ransomware 'Your personal files are encrypted' access your computer?

Ransomware ' *Your personal files are encrypted* ' is distributed through: **malicious websites** or hacked websites, and it can access your computer through the use of exploiting kits. Use the vulnerabilities on your computer to install the Trojan without your knowledge.

In addition Ransomware These ' *Your personal files are encrypted* ' can also access your computer **using spam emails attached** or links to malicious websites. **Cyber-criminals** are spam emails with fake header information, tricking users into believing it is an email from DHL or FedEx.

Or when installing a software, users invisible to install more fake software that they do not know.

2. What are Ransomware "Your personal files are encrypted"?

Ransomware " *Your personal files are encrypted* " is a **program, spyware** aimed at all Windows versions, including Windows 10, Windows Vista, Windows 8 and Windows 7.

This Ransomware type uses a special encryption method, which uses **AES-265 and RSA encryption** methods to ensure that the victim will have no choice.

When ransomware ' *Your personal files are encrypted* ' is installed on your computer, it will generate random executable names in the **% AppData** folder **"** or **% LocalAppData** directory".

This executable starts and starts scanning all drives on your computer to encrypt data files.

Ransomeware ' *Your personal files are encrypted* ' will search for files with specific extensions to encode. The files it encodes include important documents and files such as .doc, .docx, .xls, .pdf and some other files. When the file is detected, it will add a new extension to the file name (ezz, .exx, .7z.encrypted).

Below is a list of file extensions that ransomware targets:

.sql, .mp4, .7z, .rar, .m4a, .wma, .avi, .wmv, .csv, .d3dbsp, .zip, .sie, .sum, .ibank, .t13, .t12, .qdf , .gdb, .tax, .pkpass, .bc6, .bc7, .bkp, .qic, .bkf, .sidn, .sidd, .mddata, .itl, .itdb, .icxs, .hvpl, .hplg,. hkdb, .mdbackup, .syncdb, .gho, .cas, .svg, .map, .wmo, .itm, .sb, .fos, .mov, .vdf, .ztmp, .sis, .sid, .ncf, .menu, .layout, .dmp, .blob, .esm, .vcf, .vtf, .dazip, .fpk, .mlx, .kf, .iwd, .vpk, .tor, .psk, .rim, .w3x , .fsh, .ntl, .arch00, .lvl, .snx, .cfr, .ff, .vpp_pc, .lrf, .m2, .mcmeta, .vfs0, .mpqge, .kdb, .db0, .dba,. rofl, .hkx, .bar, .upk, .das, .iwi, .litemod, .asset, .forge, .ltx, .bsa, .apk, .re4, .sav, .lbf, .slm, .bik, .epk, .rgss3a, .pak, .big, wallet, .wotreplay, .xxx, .desc, .py, .m3u, .flv, .js, .css, .rb, .png, .jpeg, .txt, .p7c, .p7b, .p12, .pfx, .emem, .xt, .srw, .pef, .ptx, .r3d, .rw2, .rwl, .raw, .raf , .orf, .nrw, .mrwref, .mef, .erf, .kdc, .dcr, .cr2, .crw, .bay, .sr2, .srf, .arw, .3fr, .dng, .jpe,. jpg, .cdr, .indd, .ai, .eps, .pdf,. pdd, .psd, .dbf, .mdf, .wb2, .rtf, .wpd, .dxg, .xf, .dwg, .pst, .accdb, .mdb, .pptm, .pptx, .ppt, .xlk, .xlsb, .xlsm, .xlsx, .xls, .wps, .docm, .docx, .doc, .odb, .odc, .odm, .odp, .ods, .odt

During **file encryption** , ransomeware can create a text file for each folder with encrypted files and on Windows computers. Also ransomware can also change the wallpaper on your computer. Both the wallpaper and the text file contain the same information about how to access the payment website and how to get your files back.

In most cases, ransomeware ' *Your personal files are encrypted* ' will take control of the **.EXE** extension, when you launch an executable it will attempt to delete **Shadow Volume Copies** on the computer.

After completing the encryption of the data files, it will display the " *Your personal files are encrypted* " message at the end of your personal document, and a window with a message asking for a ransom to Decode your files.

3. Is your computer infected with the "Your personal files are encrypted" virus?

If your computer is infected with this **ransomeware** type, the background image on your Desktop will be changed and your files will be encrypted.

You will also receive the virus message " *our personal files are encrypted* ":

Your personal files are encrypted!

T?p tin b?n ?ã ???c b?o v? encrypted trên PC này: photos, videos, documents, etc. Click 'Show encrypted files' Button to view a complete list of encrypted files, and you can verify this. ?ã mã mã ? ã ???c dùng dùng m?t trình ph?c v? RSA-2048 không rõ cho máy tính này. ?? ghi t?p tin, b?n c?n ph ?i l?y khoá privately. Ch? ch? sao l?u c?a th? m?c riêng, mà cho phép b?n decrypt t?p tin c?a t?p tin, ???c ??t trên m?t secret server trong Internet; máy ch? s? g? b? th? m?c sau m?t th?i gian th?i gian ? ã xác ??nh trong c?a s? này.

N?u này ?ã ???c th?c hi?n, ai s? có th? l?y l?i.

4. Is it possible to decrypt files encrypted by ransomware "Your personal files are encrypted"?

In most cases, you cannot restore encrypted files, but you can access sites like **https://decrypter.emsisoft.com/** or **https: // id-ransomware. malwarehunterteam.com/** to decode **ransomware** .

5. The ransomware removal steps "Your personal files are encrypted"

To remove ransomware " *Your personal files are encrypted* ", follow the steps below:

Part 1: Remove ransomware "Your personal files are encrypted" from your computer

Step 1: Use Malwarebytes Anti-Malware Free to remove the "Your personal files are encrypted" virus

Malwarebytes Anti-Malware Free is a free software that supports the detection and removal of traces of malware (malware) including worms, trojans, rootkits, rogues, dialers, spyware (spyware), and some other software.

The important thing is that Malwarebytes Anti-Malware runs parallel to other antivirus software without conflict.

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

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

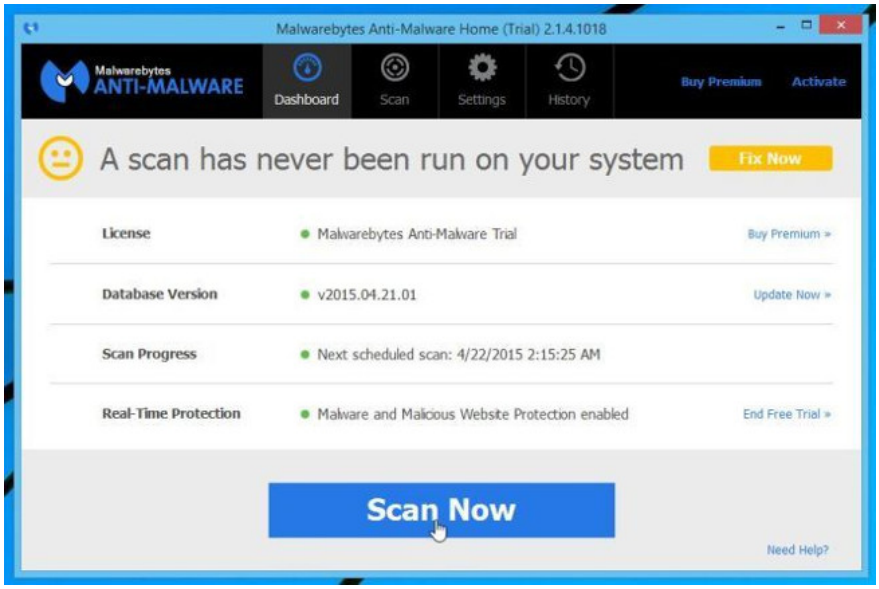
2. After downloading, close all programs, then double-click the icon named **mbam-setup** to start the Malwarebytes Anti-Malware installation process.

Now the **User Account Control** dialog box appears asking if you want to run the file. Click **Yes** to continue.

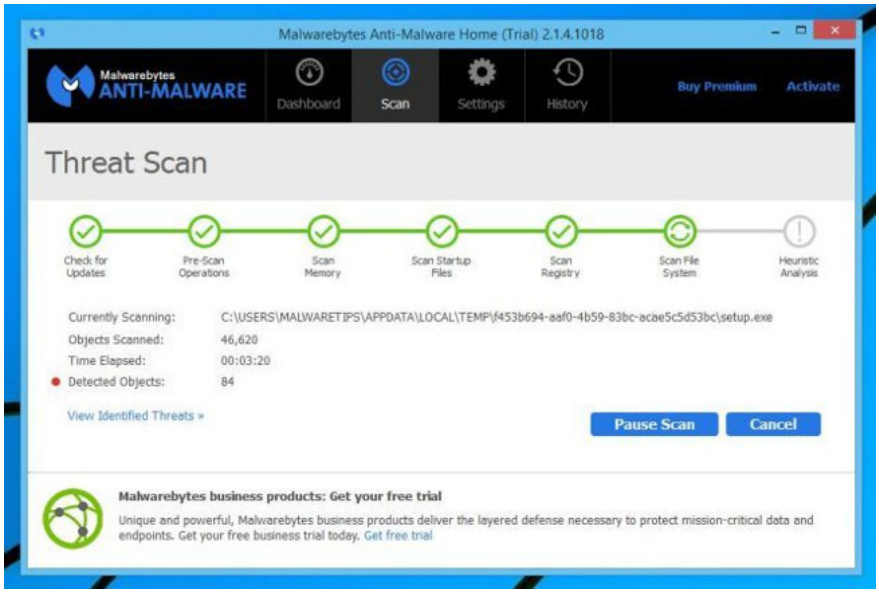
3. At the beginning of the installation process, on the screen displaying the Malwarebytes Anti-Malware Setup Wizard window, follow the on-screen instructions to install Malwarebytes Anti-Malware.

To install Malwarebytes Anti-Malware, click the **Next** button until the last window appears, click Finish.

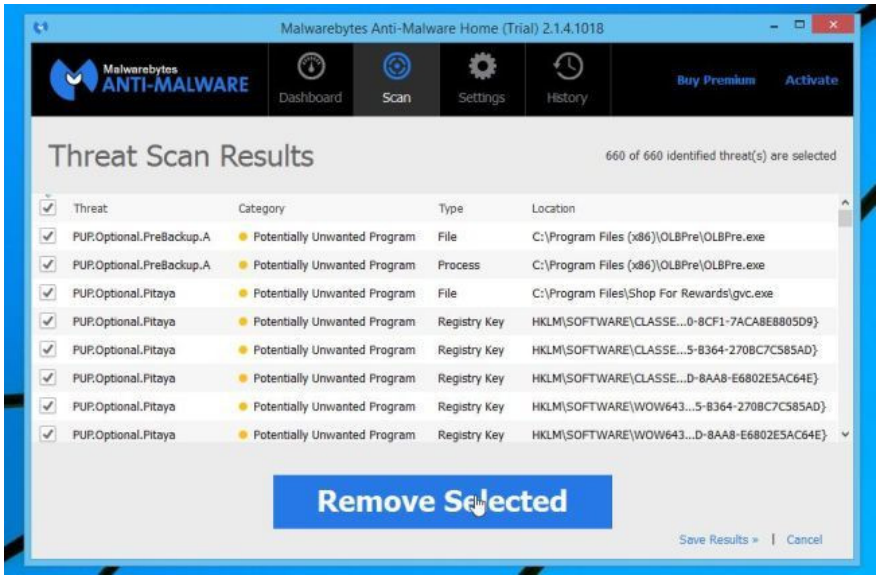
4. After installation is complete, Malwarebytes Anti-Malware will automatically open. To start the system scan, click the **Scan Now** button **.**



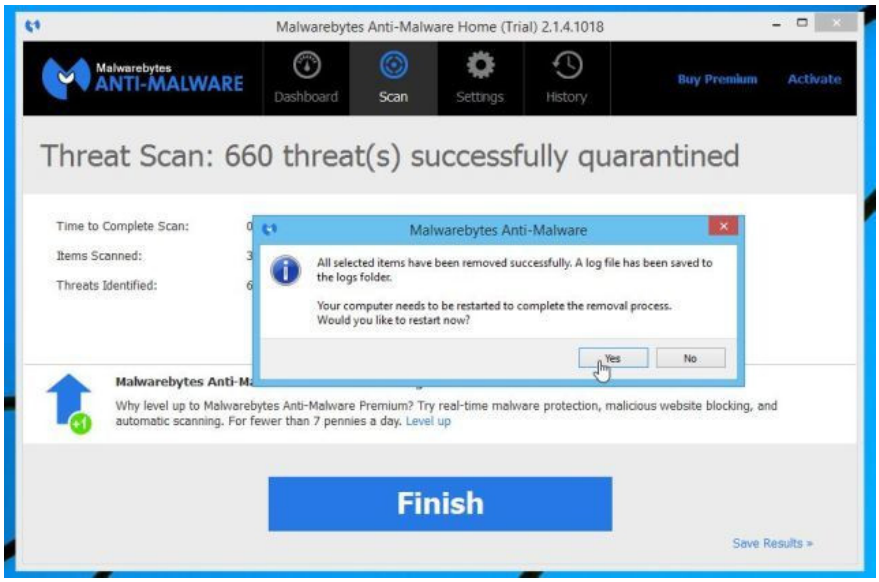
5. Malwarebytes Anti-Malware will begin scanning your computer to find and remove ransomware " *Your personal files are encrypted* ".



6. After the process finishes on the screen will appear a window displaying malware (Malware) detected by Malwarebytes Anti-Malware. To remove the software, the malicious program Malwarebytes Anti-Malware detected, click the **Remove Seletected** button.



7. Malwarebytes Anti-Malware will " *isolate* " all **malicious files** and **registry keys** detected by the program. During the process of removing these files, Malwarebytes Anti-Malware may ask you to restart the computer to complete the process. Your task is to **restart your computer** to complete the process.



Step 2: Use HitmanPro to check "double" malware "Your personal files are encrypted"

HitmanPro is designed to " *rescue* " your computer from malicious software such as viruses, trojans, rootkits, .) illegally entering the system. HitmanPro is designed to operate in parallel with other security software without causing conflict errors. The program will scan your computer within 5 minutes and will not slow down your computer.

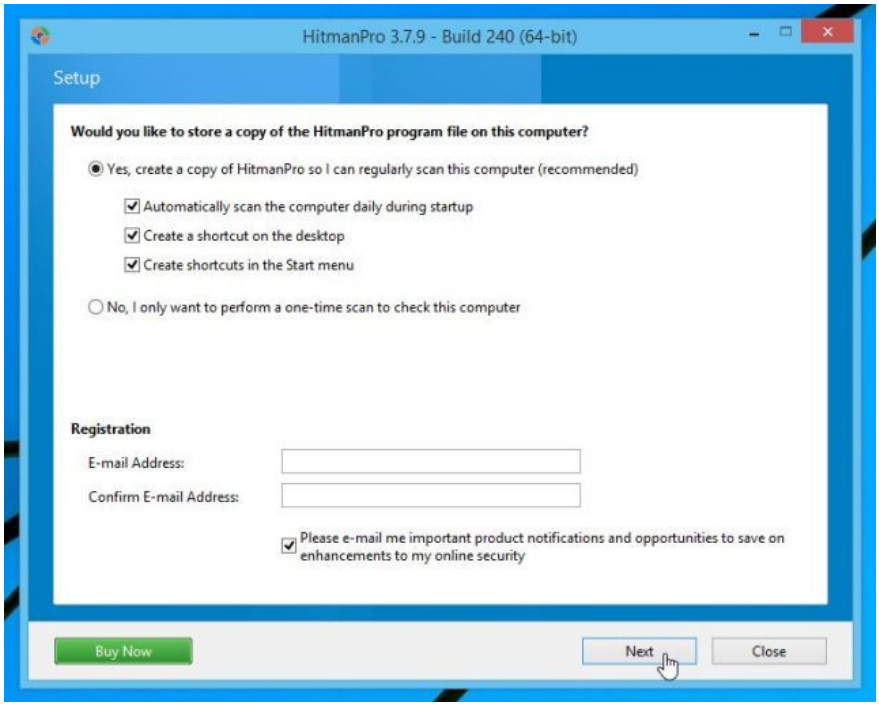
1. Download HtmanPro to your computer and install it.

Download HtmanPro to your computer and install it here.

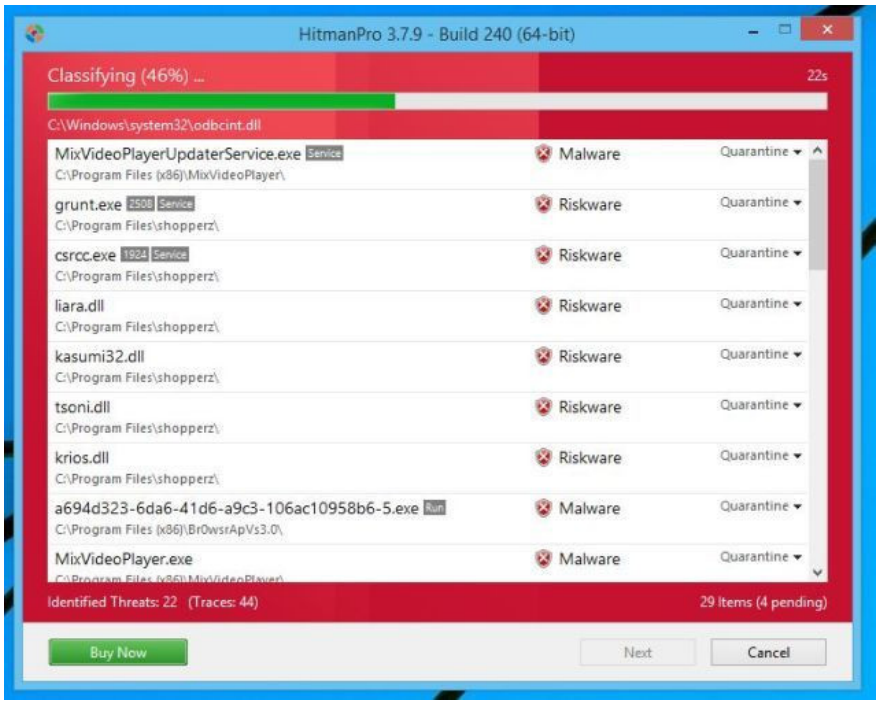
2. Double-click the file named ' *HitmanPro.exe* ' (if using 32-bit Windows version) or ' *HitmanPro_x64.exe* ' (if using 64-bit Windows version).

When the program opens, you will see the boot screen as shown below.

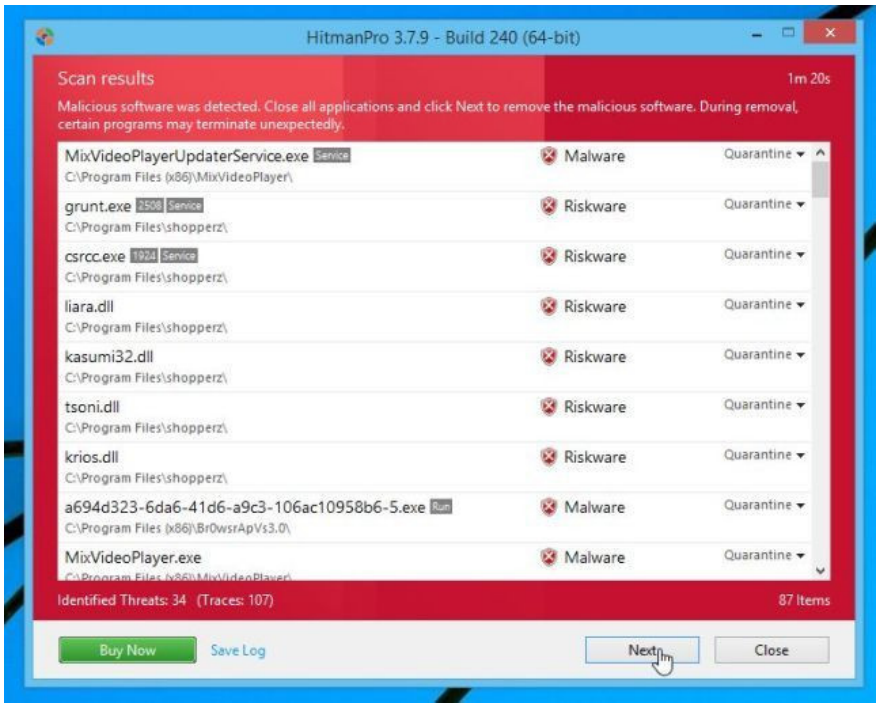
Click **Next** to install HitmanPro on your computer.



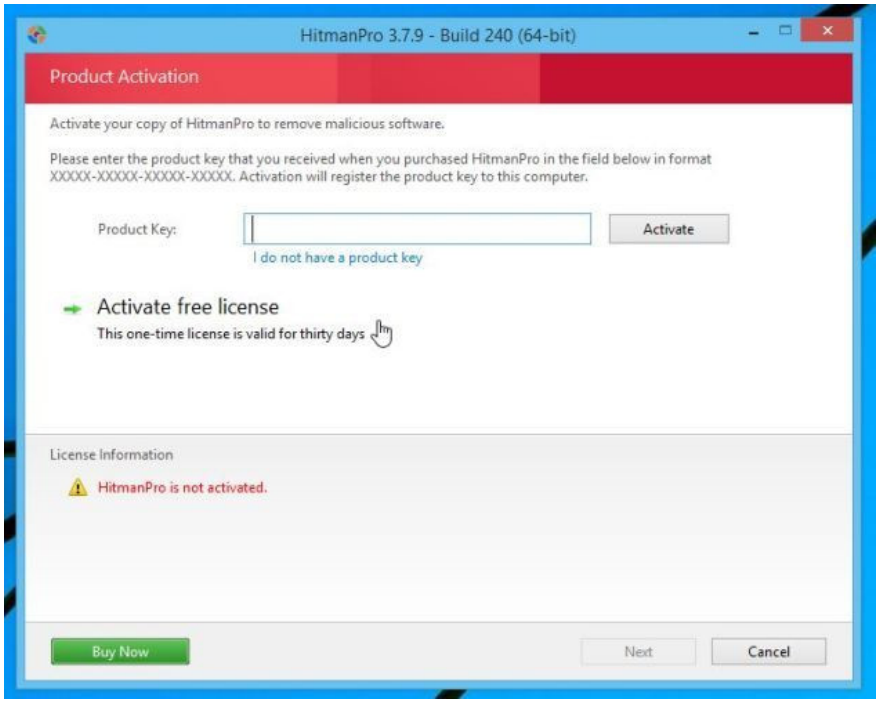
3. HitmanPro will begin the process of scanning your computer to find and remove malicious *files* ' *Your personal files are encrypted* '.



4. After the completion process on the screen will display a window containing a list of all the malicious programs HitmanPro found. Click **Next** to remove the malware " *Your personal files are encrypted* ".



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



In some cases you need to change the background and delete the dangerous file Save_Files, HELP_TO_SAVE_FILES.txt and HELP_TO_SAVE_FILES.bmp.

Part 2: Recovering files encrypted by ransomware "Your personal files are encrypted"

In some cases you can recover files encrypted by ransomware "Your personal files are encrypted" by using System Restore or other recovery software.

1. Restore encrypted files by ransomware 'Your personal files are encrypted' with ShadowExplorer

1. Download ShadowExplorer to your computer and install.

Download ShadowExplorer to your computer and install it here.

2. After downloading and installing ShadowExplorer, you can refer to the step-by-step instructions to restore files with ShadowExplorer in the video below:

In addition to ShadowExplorer you can use System Restore to recover documents that have been encrypted by ransomware.

2. Use file recovery software to recover files encrypted by ransomware "Your personal files are encrypted"

When the malicious program "Your personal files are encrypted" encrypts a file any time, the first step is to copy the file, encrypt the file it copies and delete the original file. Therefore, to fix the files that have been encrypted by ransomeware 'Your personal files are encrypted', you can use file recovery software such as:

- Recuva:

Download Recuva to your device and install it here.

Refer to steps to recover encrypted files using Recuva in the video below:

- EaseUS Data Recovery Wizard Free:

Download EaseUS Data Recovery Wizard Free to your computer and install it here.

- R-Studio:

Download R-Studio to your computer and install it here.

6. How to protect your computer from ransomeware "Your personal files are encrypted"?

To protect your computer from ransomeware " *Your personal files are encrypted* ", it is best to install **anti-virus programs** on your computer and regularly back up your personal data. Alternatively you can use some programs like HitmanPro.Alert or CryptoPrevent to prevent programs, malware (malware) from encrypting files on the system.

Refer to some of the most effective antivirus software for Windows computers here.

Refer to some of the following articles:

1. If you don't want to be a victim of Ransomware, read this article
1. To remove web ads - Social 2 Search Ads, read this article
1. Removing shortcut virus on USB has never been this simple

Good luck!

You finished reading the article "**What is the 'Your personal files are encrypted' virus? How to remove it?**" 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.