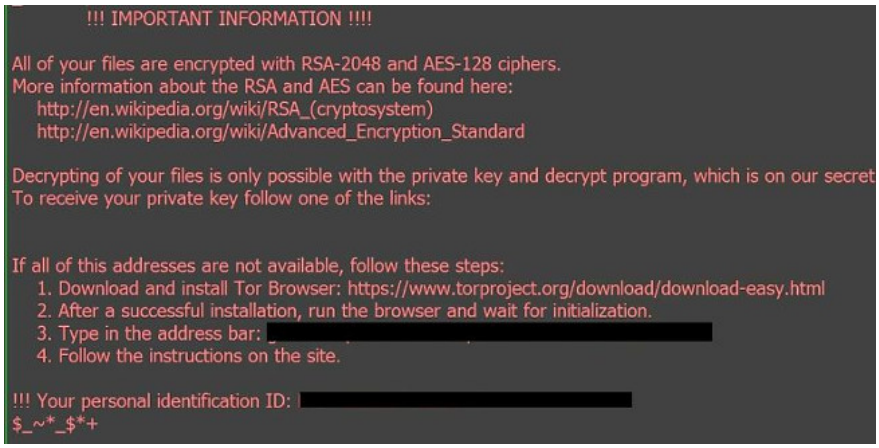
How to get rid of root virus * .OSIRIS - Ransomware Locky?

If you open any personal document and you see that document has an extension of [8_random_characters] - [4_random_characters] - [4_random_characters] - [12_random_characters] .osiris. Chances are your computer has been attacked by ransomware Locky.

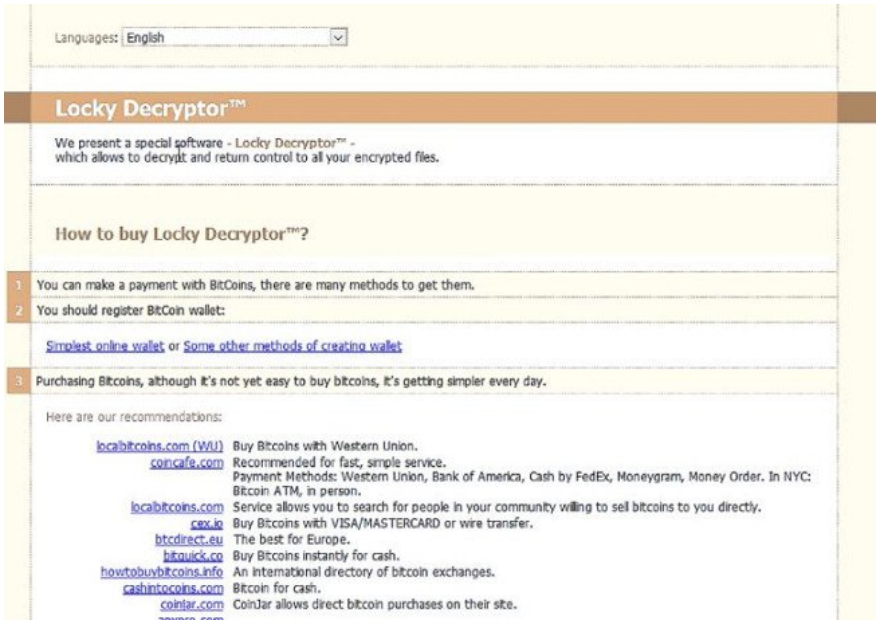
If you open any personal document and you see that document has an extension of **[8_random_characters] - [4_random_characters] - [4_random_characters] - [12_random_characters] .osiris** . Chances are your computer has been attacked by ransomware Locky.

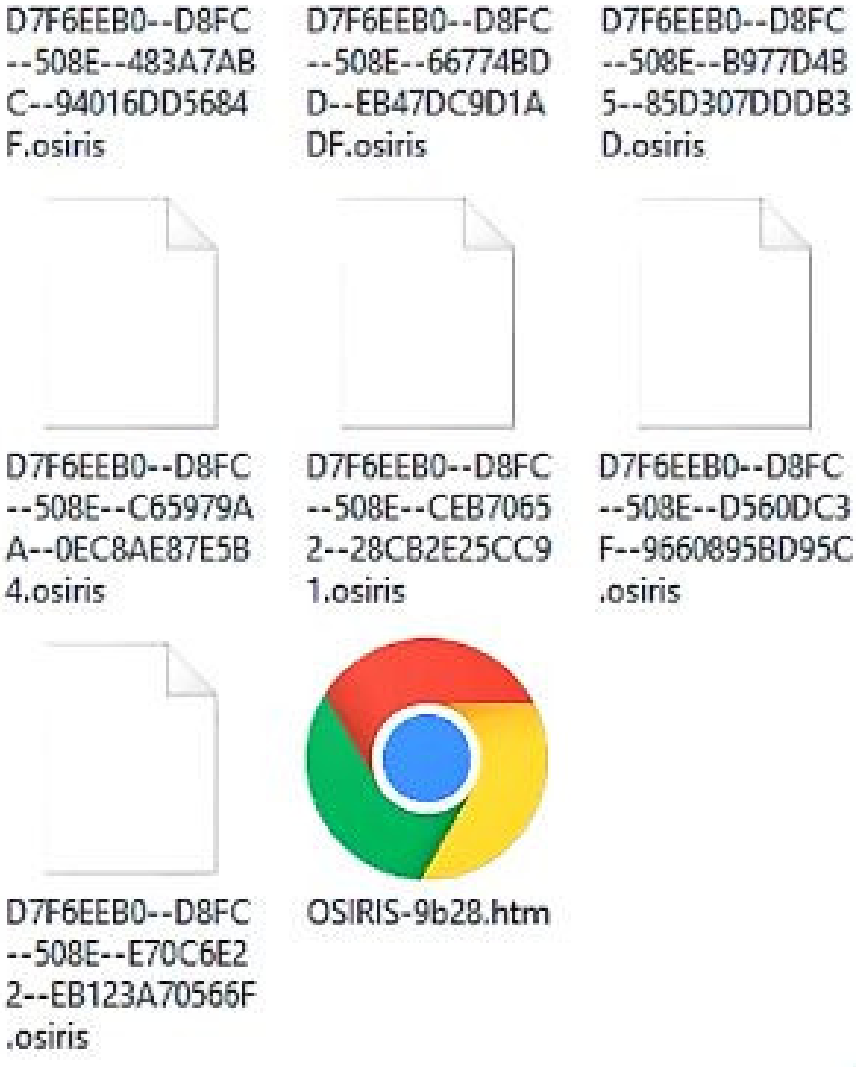
For a better understanding of ransomware, readers can refer to the information here.

Locky is a file encryption ransomware, which encrypts the personal documents it finds on the computers of the "victims" attacked by it, using RSA-2048 key (AES CBC 256 encryption algorithm). bit), then will display a message saying that to decrypt the data you need to pay about 2.5 Bitcoins, or approximately $ 1880.



The instructions are 'bundled' on victim computers in 3 files: **OSIRIS.html, OSIRIS_ [4_digit_number] .html,** and **OSIRIS.bmp.**

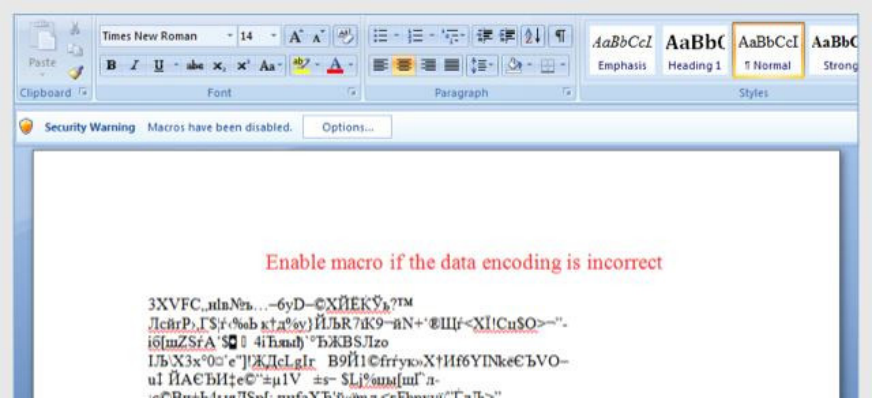

Languages: English
Locky Decryptor™
We present a special software - Locky Decryptor™ -
which allows to decrypt and return control to all your encrypted files.
How to buy Locky Decryptor™?
1 You can make a payment with BitCoins, there are many methods to get them.
2 You should register BitCoin wallet:
Simplest online wallet or Some other methods of creating wallet
3 Purchasing Bitcoins, although it's not yet easy to buy bitcoins, it's getting simpler every day.
Here are our recommendations:
localbitcoins.com (WU) Buy Bitcoins with Western Union.
coincafe.com Recommended for fast, simple service.
Payment Methods: Western Union, Bank of America, Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, in person.
localbitcoins.com Service allows you to search for people in your community willing to sell bitcoins to you directly.
cex.io Buy Bitcoins with VISA/MASTERCARD or wire transfer.
btcdirect.eu The best for Europe.
bitquick.co Buy Bitcoins instantly for cash.
howtobuybitcoins.info An international directory of bitcoin exchanges.
cashintocoins.com Bitcoin for cash.
coinjar.com CoinJar allows direct bitcoin purchases on their site.


D7F6EEB0--D8FC--508E--483A7ABC--94016DD5684F.osiris
D7F6EEB0--D8FC--508E--66774BDD--EB47DC9D1ADF.osiris
D7F6EEB0--D8FC--508E--B977D4B5--85D307DDDB3D.osiris
D7F6EEB0--D8FC--508E--C65979AA--0EC8AE87E5B4.osiris
D7F6EEB0--D8FC--508E--CEB70652--28CB2E25CC91.osiris
D7F6EEB0--D8FC--508E--D560DC3F--9660895BD95C.osiris
D7F6EEB0--D8FC--508E--E70C6E22--EB123A70566F.osiris
OSIRIS-9b28.htm

1. How does Ransomware Locky OSIRIS attack your computer?

Ransomware Locky is 'distributed' through spam containing attachments 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 is OSIRIS - ransomware Locky?

Locky ransomware is aimed at all Windows versions, including Windows 10, Windows Vista, Windows 8 and Windows 7. This Ransomware type uses special user-specific encryption of files that it uses. AES-265 and RSA encryption methods to ensure that the victim will have no choice.

When ransomware Locky 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 Lock will search for files with specific extensions to encrypt. 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

After the files are encrypted with the extension .osiris, ransomeware Locky can create an **OSIRIS.html, OSIRIS_ [4_digit_number] .html** , or **OSIRIS.bmp files** for each folder with encrypted files and on Windows computers.

These files are located in each folder containing the encrypted files as well as in the Startup folder, the folder containing the programs that are automatically displayed when the user logs in. These files will contain information on how to access payment sites and get back your files.

In most cases, ransomeware Locky will take control of the .EXE extension, when you launch an executable it will attempt to delete Shadow Volume Copies on the computer.

After finishing encrypting the data files, it will delete all Shadow Volume Copies on your computer. It does not allow users to use Shadow Volume Copies to restore (encrypted) files.

3. Does your computer have Ransomware Locky - OSIRIS attack?

When ransomeware Lock attacks your computer, it scans all the drives on the system to find the files it targets, encrypts them and adds the .osiris extension to the files.

After the files are encrypted, you cannot open these files with programs like you normally would. Also when ransomware Locky ends the victim's file encryption process, it will also change the wallpaper on the victim's computer.

In addition it will also display a ransom note as HTML on your default browser. These notes include how to instruct how to connect to the Decrypt Service, where you can learn more about what happened to your files and how to pay.

Ransomware Locky will display a message:

IMPORTANT INFORMATION !!!!

T?t c? các t?p tin là t?p tin ?ã ch?a v?i RSA-2048 and AES-128 ciphers.

Thông tin thêm v? RSA và AES có th? tìm th?y này:

hxxps: //en.wikipedia.org/wiki/RSA_ (cryptosystem)

hxxps: //en.wikipedia.org/wiki/Advanced_Encryption_Standard

Không th? gi?i mã m?t t?p tin t?p tin này có th? v?i ch??ng trình privately và decrypt ch??ng trình,
nó trên máy ch? Secret

?? l?y thông báo theo ?ây theo m?t c?a các liên k?t:

[edited]

N?u t?t c? các ??a ch? này không s?n sàng, theo ?ây Steps:

1. Download and install Tor Browser: hxxps: //www.torproject.org/download/download-easy.html

2. Sau khi cài ??t vi?c cài ??t, ch?y browser và ch? cho ??u ??u.

3. Type in the address bar: [edited]

4. Follow instructions on the site.

!!! Your personal identification ID: [edited]

4. Is it possible to decrypt files encrypted by ransomware Locky?

Up to this point, it is not possible to recover files encrypted by the .osiris extension.

The most notable point of ransomware Locky is how it encrypts user files. Specifically, it uses AES-265 and RSA encryption methods - to ensure that users 'attacked' have no choice but to purchase a private key.

The RSA public key can be decrypted with its corresponding private key. The reason because AES key is hidden when using RSA encryption and private RSA key is not available, decrypting the file is not feasible.

And because there must be a private key to unlock the encrypted files, these keys are available through cyber criminals, so victims can be tempted to buy and pay one. exorbitant fees.

4.1. Use software to recover encrypted files by ransomware Locky

Option 1: Use ShadowExplorer to recover encrypted files by ransomware Locky

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:

Option 2. Use file recovery software to recover files encrypted by the .osiris extension

When the extension .osiris 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 information that has been encrypted by the .osiris extension, you can use file recovery software such as:

1. Recuva:

Download Recuva to your device and install it here.

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

1. EaseUS Data Recovery Wizard Free:

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

1. R-Studio:

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

5. How to remove .osiris extension?

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.

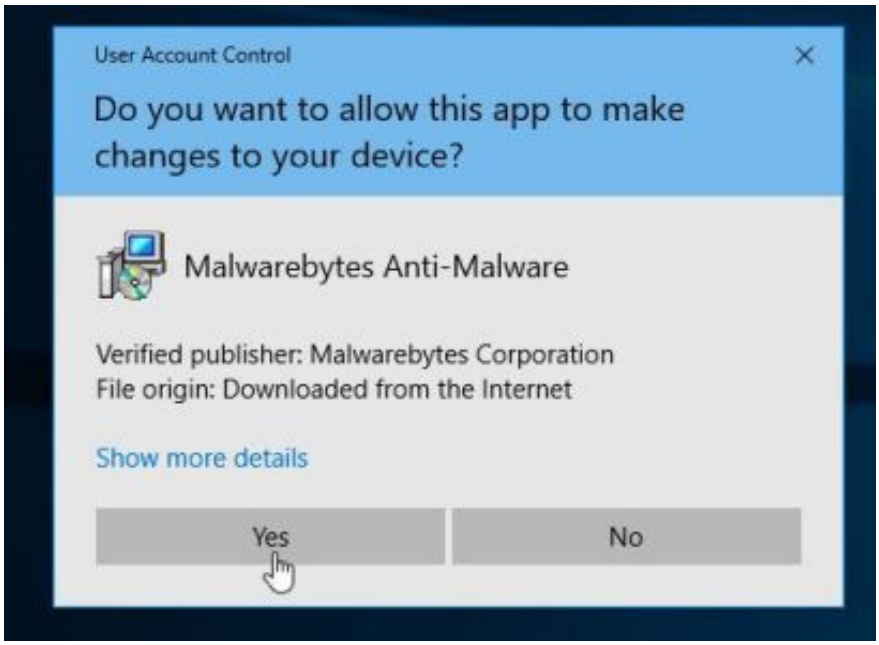
The important thing is that Malwarebytes Anti-Malware runs parallel to other antivirus software without conflict.

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

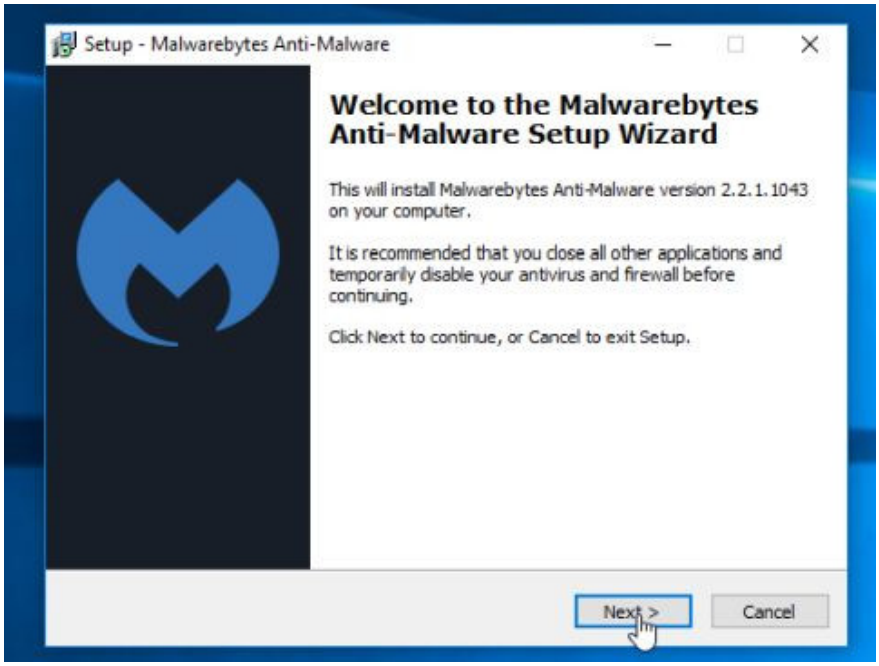
Download Malwarebytes Anti-Malware Free to your computer and install it here.

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.

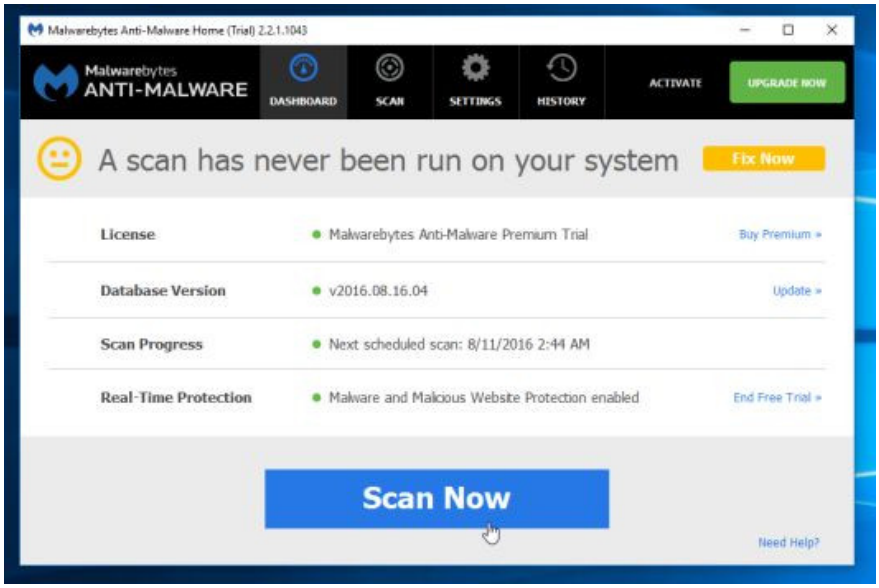


3. At the beginning of the installation process, on the screen displaying the Malwarebytes Anti-Malware Setup Wizard window, follow the on-screen instructions to install Malwarebytes Anti-Malware.

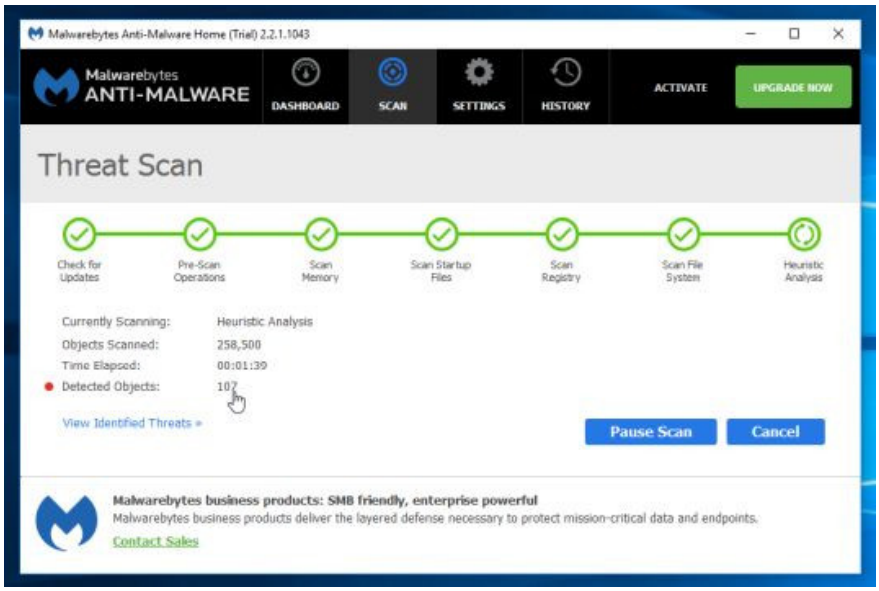


To install Malwarebytes Anti-Malware, click the **Next** button until the last window appears, click **Finish.**

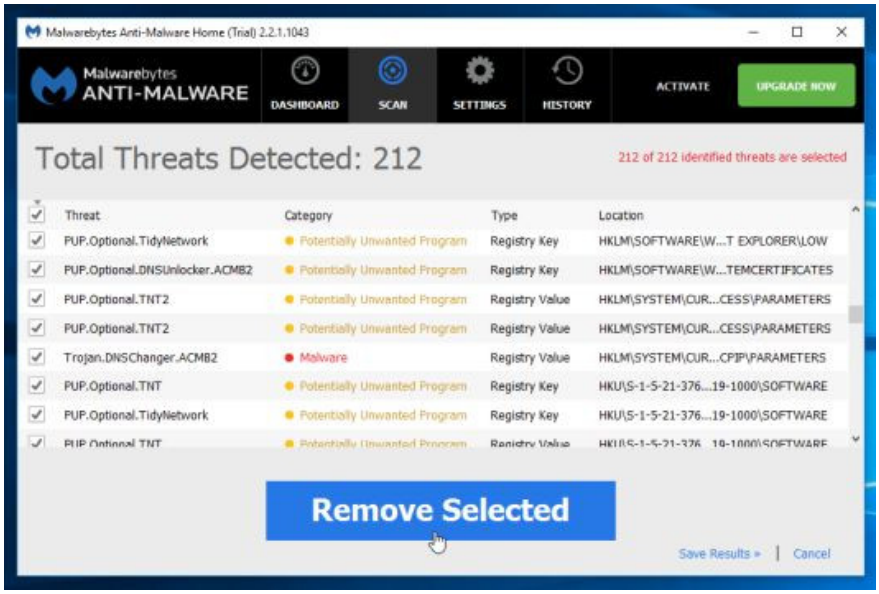
4. After installation is complete, Malwarebytes Anti-Malware will automatically open. To start the system scan, click the **Scan Now** button **.**



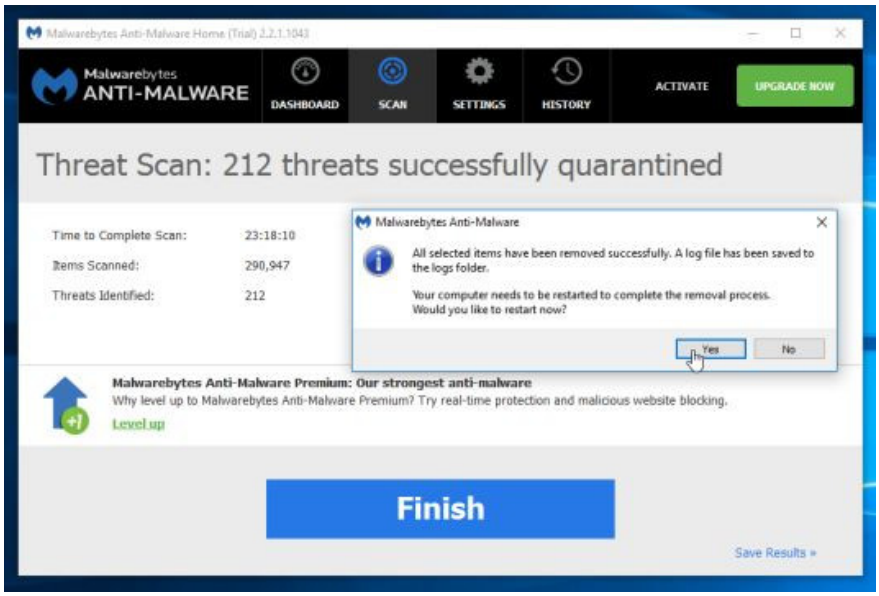
5. Malwarebytes Anti-Malware will begin the process of scanning your computer to find and remove .osiris malware.



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 remove ransomware Locky

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.

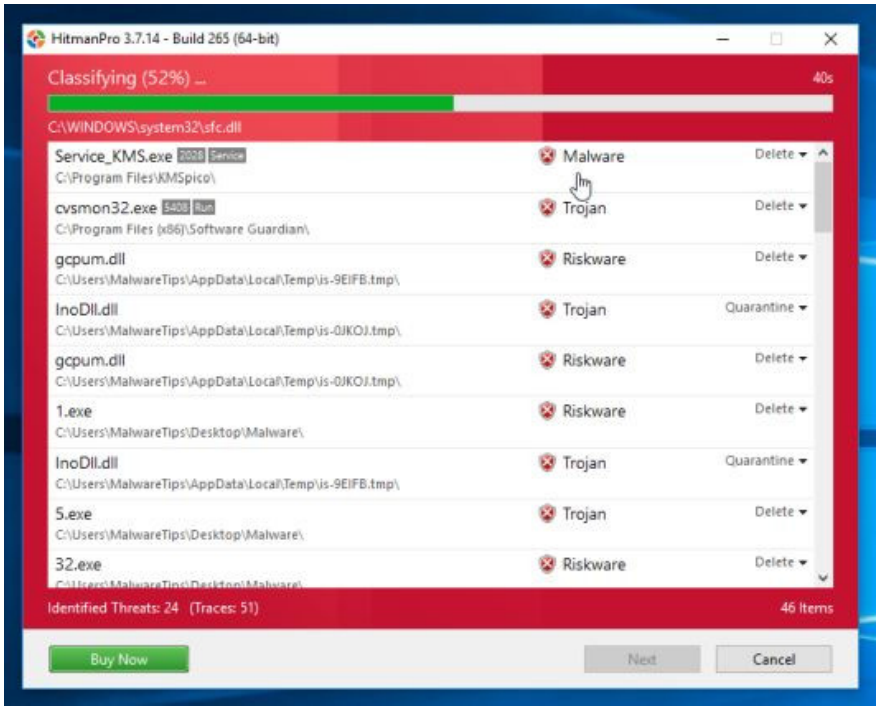
1. Download HtmanPro to your computer and install it.

Download HtmanPro to your computer and install it here.

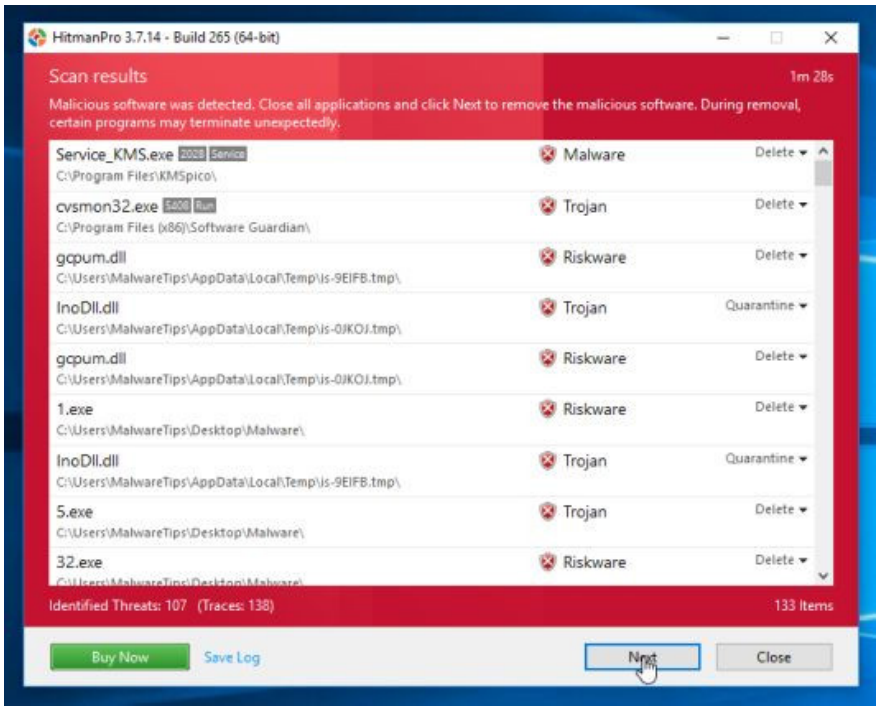
2. Double-click the file named ' *HitmanPro.exe* ' (if using 32-bit Windows version) or ' *HitmanPro_x64.exe* ' (if using 64-bit Windows version).

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

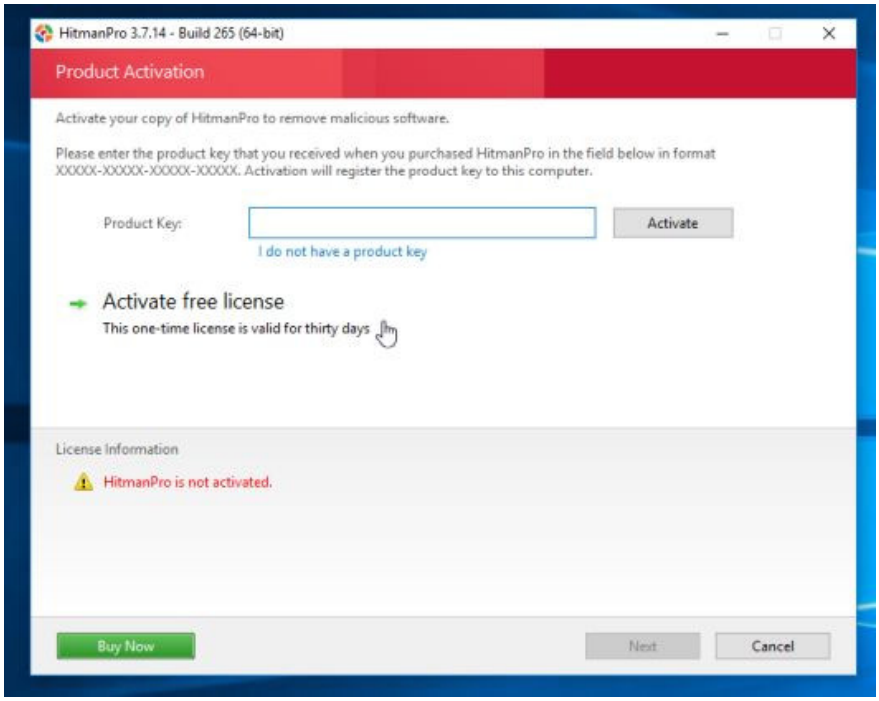
3. HitmanPro will begin the process of scanning your computer to find and remove malicious files.



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 on your system.



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



6. How to protect your computer from Locky ransomeware?

To protect your computer from ransomeware Locky, it is best to install **anti-virus programs** on your computer and regularly back up your personal data. Also you can use some programs like HitmanPro.Alert to prevent programs, malware (malware) encrypt files on the system.

Refer to the steps to download and install HitmanPro.Alert in the video below:

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

Refer to some of the following articles:

1. What to do to handle "No Internet After Malware Removal" error?

1. How to remove unwanted Toolbar on Chrome, Firefox, IE and Edge browsers?

1. The steps to clean up the virus 'Activate this edition of Windows' attack your Windows computer

Good luck!

You finished reading the article "**How to get rid of root virus * .OSIRIS - Ransomware Locky?**" 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.
