Remove RRBB Ransomware Free Download

Remove RRBB Ransomware Free Download.. How to Remove RRBB Ransomware (Virus Removal Guide) Download

Rating: Not Rated Yet
Price

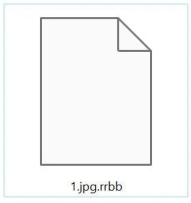
Report Copyright about this product

Description

Remove RRBB Ransomware Free Download

How to Remove RRBB Ransomware (Virus Removal Guide)
RRBB is a file-encrypting ransomware infection that restricts access to data (documents, images, videos) by encrypting files with the ".rrbb" extension. This guide teaches you how to remove the RRBB ransomware virus by following easy step-by-step instructions.

If you cannot open your images, documents, or files and they have a .rrbb extension, then your computer is infected with the STOP/DJVU ransomware.
This ransomware encrypts the personal documents found on the victim's computer with the ".rrbb" extension, then displays a message which offers to decrypt the data if payment in Bitcoin is made. The instructions are placed on the victim's desktop in the "_readme.txt" file.



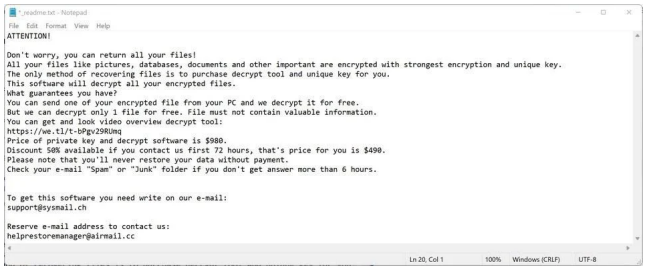


Image: RRBB Ransomware Encrypted Files

What is the RRBB ransomware?

RRBB is a file-encrypting ransomware infection that restricts access to data (documents, images, videos) by encrypting files with the “.rrbb” extension. It then attempts to extort money from victims by asking for “ransom”, in the form of Bitcoin cryptocurrency, in exchange for access to data.

When you are first infected with the RRBB ransomware it will scan your computer for images, videos, and important productivity documents and files such as .doc, .docx, .xls, .pdf. When these files are detected, the ransomware will encrypt them and change their extension to “.rrbb”, so that you are no longer able to open them.

Once the RRBB ransomware has encrypted the files on your computer, it will display the “_readme.txt” file that contains the ransom note and instructions on how to contact the authors of this ransomware. The victims of this ransomware will be asked to contact these malware developers via the This email address is being protected from spambots. You need JavaScript enabled to view it. document.getElementById('cloakc0da08d93c452b5c6dbcf52c52a8a0cc').innerHTML = ''; var prefix = 'ma' + 'il' + 'to'; var path = 'hr' + 'ef' + '='; var addyc0da08d93c452b5c6dbcf52c52a8a0cc = 'support' + '@'; addyc0da08d93c452b5c6dbcf52c52a8a0cc = addyc0da08d93c452b5c6dbcf52c52a8a0cc + 'sysmail' + '.' + 'ch'; var addy_textc0da08d93c452b5c6dbcf52c52a8a0cc = 'support' + '@' + 'sysmail' + '.' + 'ch';document.getElementById('cloakc0da08d93c452b5c6dbcf52c52a8a0cc').innerHTML += ''+addy_textc0da08d93c452b5c6dbcf52c52a8a0cc+''; and This email address is being protected from spambots. You need JavaScript enabled to view it. document.getElementById('cloak0a532e1d7600f236a037e870c203e50b').innerHTML = ''; var prefix = 'ma' + 'il' + 'to'; var path = 'hr' + 'ef' + '='; var addy0a532e1d7600f236a037e870c203e50b = 'helprestoremanager' + '@'; addy0a532e1d7600f236a037e870c203e50b = addy0a532e1d7600f236a037e870c203e50b + 'airmail' + '.' + 'cc'; var addy_text0a532e1d7600f236a037e870c203e50b = 'helprestoremanager' + '@' + 'airmail' + '.' + 'cc';document.getElementById('cloak0a532e1d7600f236a037e870c203e50b').innerHTML += ''+addy_text0a532e1d7600f236a037e870c203e50b+''; email addresses.

This is the ransom note that the RRBB ransomware will show to its victims:

ATTENTION!

Don’t worry, you can return all your files!
All your files like pictures, databases, documents and other important are encrypted with strongest encryption and unique key.
The only method of recovering files is to purchase decrypt tool and unique key for you.

This software will decrypt all your encrypted files.
What guarantees you have?

You can send one of your encrypted file from your PC and we decrypt it for free.

But we can decrypt only 1 file for free. File must not contain valuable information.

You can get and look video overview decrypt tool:
https://we.tl/t-bPgv29RUmq

Price of private key and decrypt software is $980.
Discount 50% available if you contact us first 72 hours, that’s price for you is $490.

Please note that you’ll never restore your data without payment.
Check your e-mail “Spam” or “Junk” folder if you don’t get answer more than 6 hours.

To get this software you need write on our e-mail:
This email address is being protected from spambots. You need JavaScript enabled to view it. document.getElementById('cloak060b36fa39a50ef1845e1627da857463').innerHTML = ''; var prefix = 'ma' + 'il' + 'to'; var path = 'hr' + 'ef' + '='; var addy060b36fa39a50ef1845e1627da857463 = 'support' + '@'; addy060b36fa39a50ef1845e1627da857463 = addy060b36fa39a50ef1845e1627da857463 + 'sysmail' + '.' + 'ch'; var addy_text060b36fa39a50ef1845e1627da857463 = 'support' + '@' + 'sysmail' + '.' + 'ch';document.getElementById('cloak060b36fa39a50ef1845e1627da857463').innerHTML += ''+addy_text060b36fa39a50ef1845e1627da857463+'';

Reserve e-mail address to contact us:
This email address is being protected from spambots. You need JavaScript enabled to view it. document.getElementById('cloak4b5aa80aba63e16a83ee5d5af902f3a7').innerHTML = ''; var prefix = 'ma' + 'il' + 'to'; var path = 'hr' + 'ef' + '='; var addy4b5aa80aba63e16a83ee5d5af902f3a7 = 'helprestoremanager' + '@'; addy4b5aa80aba63e16a83ee5d5af902f3a7 = addy4b5aa80aba63e16a83ee5d5af902f3a7 + 'airmail' + '.' + 'cc'; var addy_text4b5aa80aba63e16a83ee5d5af902f3a7 = 'helprestoremanager' + '@' + 'airmail' + '.' + 'cc';document.getElementById('cloak4b5aa80aba63e16a83ee5d5af902f3a7').innerHTML += ''+addy_text4b5aa80aba63e16a83ee5d5af902f3a7+'';

Here is a summary of the RRBB ransomware:

Ransomware family: STOP/DJVU ransomware
Extensions: .rrbb
Ransomware note: _readme.txt
Ransom: From $490 to $980 (in Bitcoins)
Contact: This email address is being protected from spambots. You need JavaScript enabled to view it.
document.getElementById('cloak10007993ef34637338b262651942483c').innerHTML = ''; var prefix = 'ma' + 'il' + 'to'; var path = 'hr' + 'ef' + '='; var addy10007993ef34637338b262651942483c = 'support' + '@'; addy10007993ef34637338b262651942483c = addy10007993ef34637338b262651942483c + 'sysmail' + '.' + 'ch'; var addy_text10007993ef34637338b262651942483c = 'support' + '@' + 'sysmail' + '.' + 'ch';document.getElementById('cloak10007993ef34637338b262651942483c').innerHTML +=
''+addy_text10007993ef34637338b262651942483c+''; and This email address is being protected from spambots. You need JavaScript enabled to view it. document.getElementById('cloakf04b038b8a1df7c89f3f5816090c0283').innerHTML = ''; var prefix = 'ma' + 'il' + 'to'; var path = 'hr' + 'ef' + '='; var addyf04b038b8a1df7c89f3f5816090c0283 = 'helprestoremanager' + '@'; addyf04b038b8a1df7c89f3f5816090c0283 = addyf04b038b8a1df7c89f3f5816090c0283 + 'airmail' + '.' + 'cc'; var addy_textf04b038b8a1df7c89f3f5816090c0283 = 'helprestoremanager' + '@' + 'airmail' + '.' + 'cc';document.getElementById('cloakf04b038b8a1df7c89f3f5816090c0283').innerHTML += ''+addy_textf04b038b8a1df7c89f3f5816090c0283+'';
Symptoms: The images, videos, and other documents have the ".rrbb" extension and cannot be opened by any programs

How did the RRBB ransomware get on my computer?

The RRBB ransomware is distributed via spam email containing infected attachments or by exploiting vulnerabilities in the operating system and installed programs.

Here's how the RRBB ransomware might get on your computer:

Cfhkf-criminals spam out an email, with forged header information, tricking you into believing that it is from a shipping company like DHL or FedEx. The email tells you that they tried to deliver a package to you, but failed for some reason. Sometimes the emails claim to be notifications of a shipment you have made. Either way, you can't resist being curious as to what the email is referring to – and open the attached file (or click on a link inside the email). And with that, your computer is infected with the RRBB ransomware.

The RRBB ransomware was also observed attacking victims by exploiting vulnerabilities in the program installed on the computer or the operating system itself. Commonly exploited software includes the operating system itself, browsers, Microsoft Office, and third-party applications.

Remove the RRBB ransomware and recover the files

It's important to understand that by starting the removal process you risk losing your files, as we cannot guarantee that you will be able to recover them. Your files may be permanently compromised when trying to remove this infection or trying to recover the encrypted documents.

We cannot be held responsible for losing your files or documents during this removal process.
It's recommended to create a backup image of the encrypted drives before proceeding with the malware removal instructions.

This malware removal guide may appear overwhelming due to the number of steps and numerous programs that are being used. We have only written it this way to provide clear, detailed, and easy-to-understand instructions that anyone can use to remove malware for free.
Please perform all the steps in the correct order.

To remove the RRBB ransomware, follow these steps:

STEP 1: Start your computer in Safe Mode with Networking

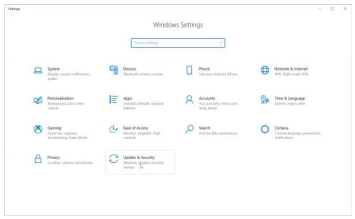
In this first step, we will start your computer in Safe Mode with Networking to prevent RRBB malicious drivers and services from

loading at Windows start-up. We're using Safe mode because it starts Windows in a basic state, using a limited set of files and drivers.

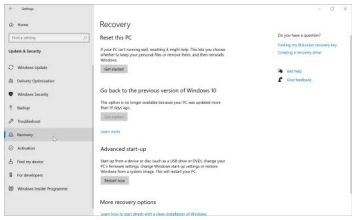
FOR WIN 10

Before you enter Safe Mode, you need to enter the Windows Recovery Environment (winRE). To do this, follow the below steps:

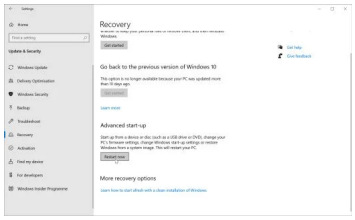
1. Press the Windows logo key + I on your keyboard to open Settings. If that doesn't work, select the Start button, then select Settings.



2. When the Windows Settings window opens, select Update & Security, then click on Recovery.

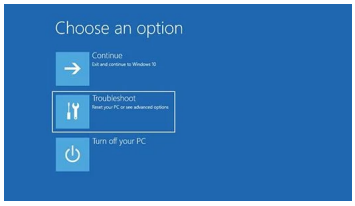


3. Under Advanced startup, select Restart now.

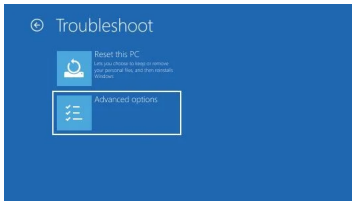


Now that you are in Windows Recovery Environment, you will follow these steps to take you to safe mode:

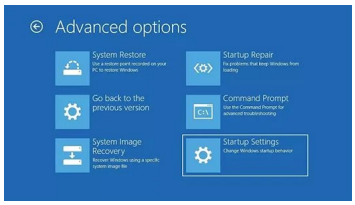
1. On the Choose an option screen, select "Troubleshoot".



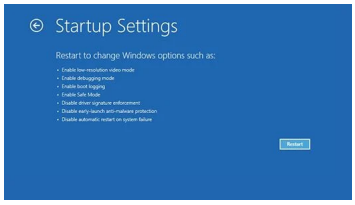
2. On the "Troubleshoot" screen, click the "Advanced Options" button.



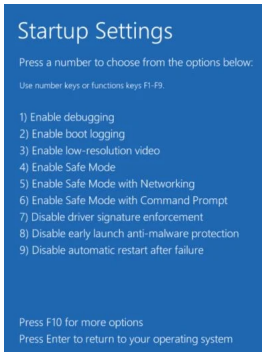
3. On the "Advanced Options" page, click the "Startup Settings" option. In Windows 8, this option is labeled "Windows Startup Settings" instead.



4. On the “Startup Settings” page, click the “Restart”.



5. After your device restarts, you’ll see a list of options. Select option 5 from the list or press F5 to enter Safe Mode with Networking.



6. While your computer is running in Safe Mode with Networking, we will need to download, install and run a scan with Malwarebytes (explained in Step 2).

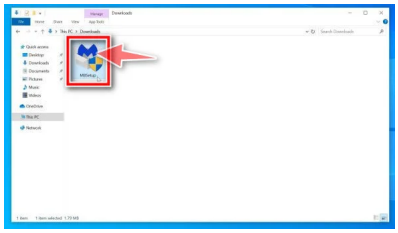
STEP 2: Use Malwarebytes to remove RRBB ransomware

While the computer is in Safe Mode with Networking, we will download, install and run a system scan with Malwarebytes.

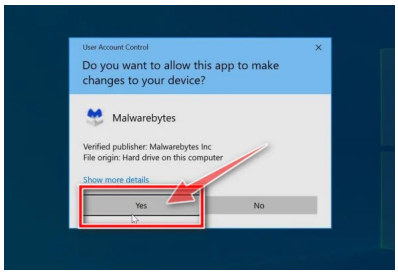
Malwarebytes Free is one of the most popular and most used anti-malware software for Windows, and good reasons. It is able to destroy many types of malware that other software tends to miss, without costing you absolutely nothing. When it comes to cleaning up an infected device, Malwarebytes has always been free and we recommend it as an essential tool in the fight against malware.

1. Download Malwarebytes.
You can download Malwarebytes for Windows by clicking download button.

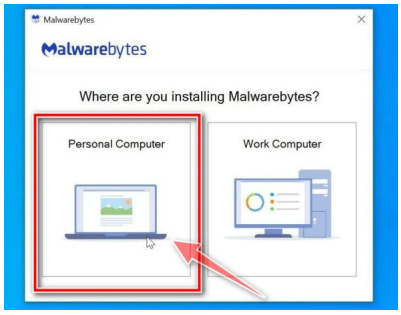
2. Double-click on the Malwarebytes setup file.
When Malwarebytes has finished downloading, double-click on the MBSetup file to install Malwarebytes on your computer. In most cases, downloaded files are saved to the Downloads folder.



You may be presented with a User Account Control pop-up asking if you want to allow Malwarebytes to make changes to your device. If this happens, you should click “Yes” to continue with the Malwarebytes installation.



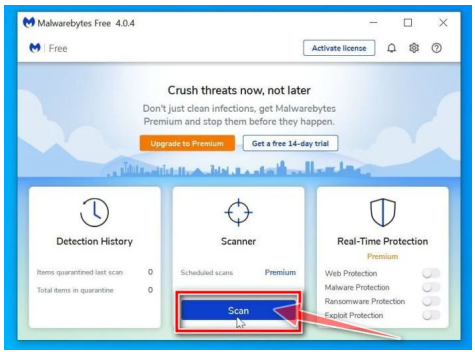
3. Follow the on-screen prompts to install Malwarebytes.
When the Malwarebytes installation begins, you will see the Malwarebytes setup wizard which will guide you through the installation process. The Malwarebytes installer will first ask you what type of computer are you installing this program on, click either Personal Computer or Work Computer.



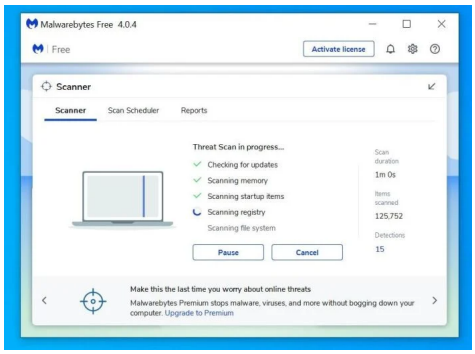
On the next screen, click “Install” to install Malwarebytes on your computer.

When your Malwarebytes installation completes, the program opens to the Welcome to Malwarebytes screen. Click the “Get started” button.

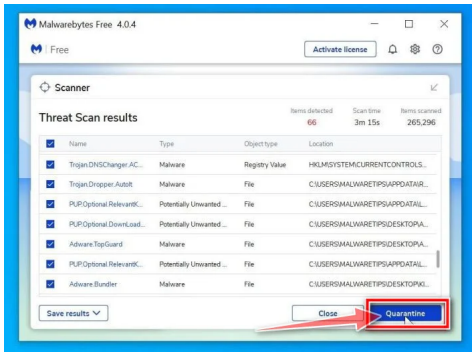
4. Click on “Scan”.
To scan your computer with Malwarebytes, click on the “Scan” button. Malwarebytes will automatically update the antivirus database and start scanning your computer for malware.



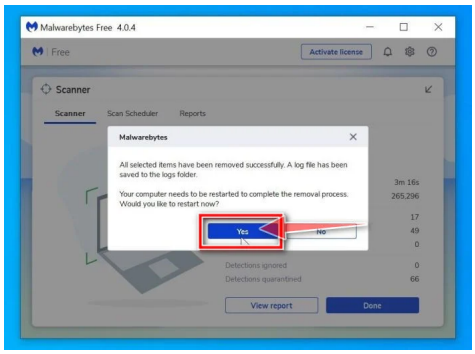
5. Wait for the Malwarebytes scan to complete.
Malwarebytes will scan your computer for the RRBB malware and other malicious programs. This process can take a few minutes, so we suggest you do something else and periodically check on the status of the scan to see when it is finished.



6. Click on “Quarantine”.
When the scan has been completed, you will be presented with a screen showing the malware infections that Malwarebytes has detected. To remove the RRBB malicious files that Malwarebytes has found, click on the “Quarantine” button.



7. Restart computer.
Malwarebytes will now remove the RRBB ransomware malware and other malicious programs that it has found. To complete the malware removal process, Malwarebytes will ask you to restart your computer.



When the malware removal process is complete, your computer should start in normal mode (if not, simply restart your device to exit Safe Mode) and continue with the rest of the instructions. We do recommend that you run another scan with Malwarebytes once you’re in Normal mode to make sure all the malicious files were removed.

STEP 3: Scan and clean your computer with HitmanPro

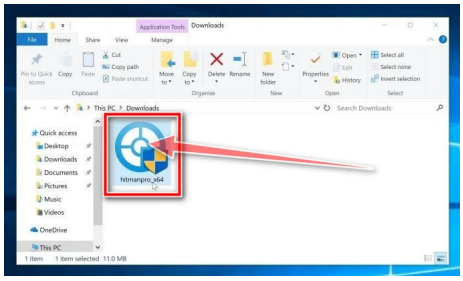
In this third step, while the computer is in normal back, we will download and run a scan with HitmanPro to remove the RRBB ransomware and other malicious programs.

HitmanPro is a second opinion scanner that takes a unique cloud-based approach to malware scanning. HitmanPro scans the behavior of active files and also files in locations where malware normally resides for suspicious activity. If it finds a suspicious file that’s not already known, HitmanPro sends it to its clouds to be scanned by two of the best antivirus engines today, which are Bitdefender and Kaspersky.

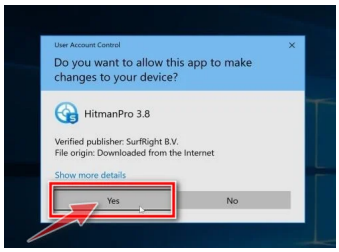
Although HitmanPro is shareware and costs $24.95 for 1 year on 1 PC, there is actually no limit on scanning. The limitation only kicks in when there is a need to remove or quarantine detected malware by HitmanPro on your system and by then, you can activate the one-time 30-days trial to enable the clean up.

1. Download HitmanPro.
You can download HitmanPro by clicking download button.

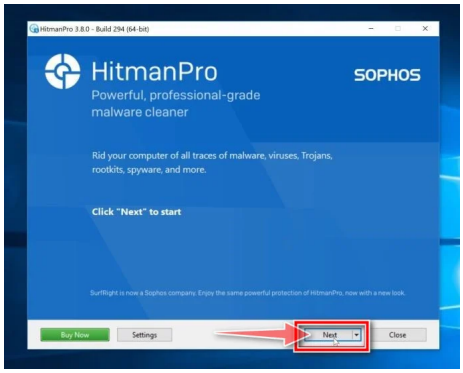
2. Install HitmanPro.
When HitmanPro has finished downloading, double-click on “hitmanpro.exe” (for 32-bit versions of Windows) or “hitmanpro_x64.exe” (for 64-bit versions of Windows) to install this program on your PC. In most cases, downloaded files are saved to the *Downloads folder*.

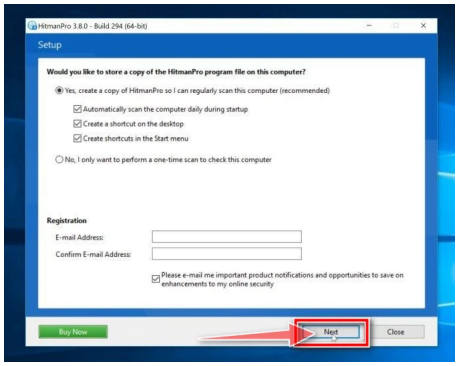


You may be presented with a User Account Control pop-up asking if you want to allow HitmanPro to make changes to your device. If this happens, you should click “Yes” to continue with the installation.

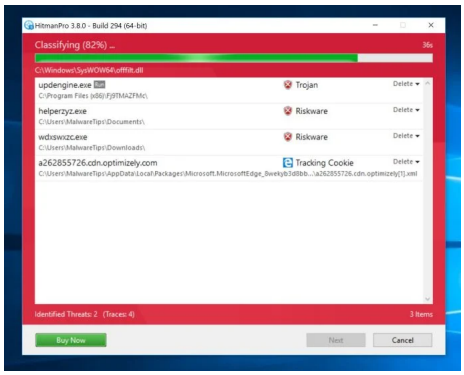


3. Follow the on-screen prompts.
When HitmanPro starts you will be presented with the start screen as shown below. Click on the “Next” button to perform a system scan.

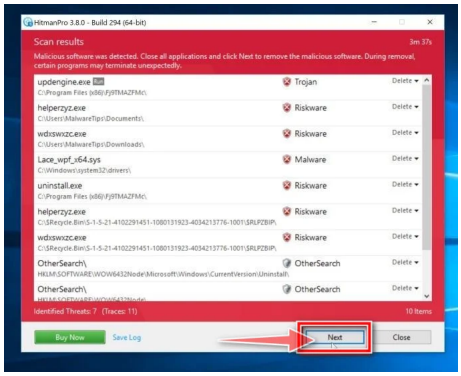




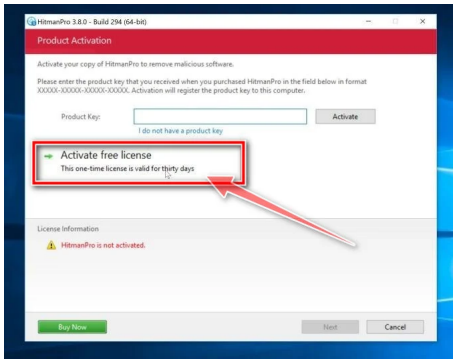
4. Wait for the HitmanPro scan to complete.
HitmanPro will now begin to scan your computer for the RRBB ransomware and other malicious programs. This process will take a few minutes.

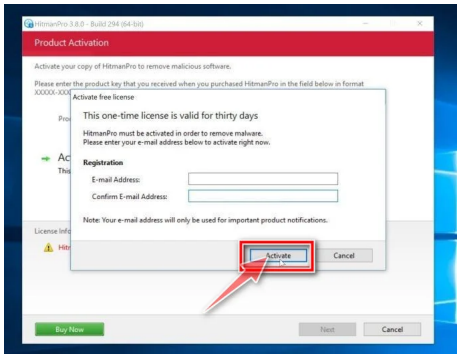


5. Click on “Next”.
When HitmanPro has finished the scan, it will display a list of all the malware that the program has found. Click on the “Next” button to remove the RRBB ransomware and other malicious programs.



6. Click on “Activate free license”.
Click on the “Activate free license” button to begin the free 30 days trial and remove the RRBB ransomware and other malicious files from the computer.





When the process is complete, you can close HitmanPro and continue with the rest of the instructions.

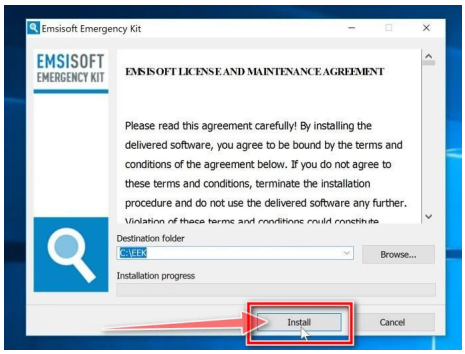
STEP 4: Double-check for malicious programs with Emsisoft Emergency Kit

In this fourth step, we will scan the computer with Emsisoft Emergency Kit to remove any leftover files from the RRBB ransomware and other malicious programs.
While the Malwarebytes and HitmanPro scans are more than enough, we're recommending Emsisoft Emergency Kit to users who still have malware-related issues or just want to make sure their computer is 100% clean.

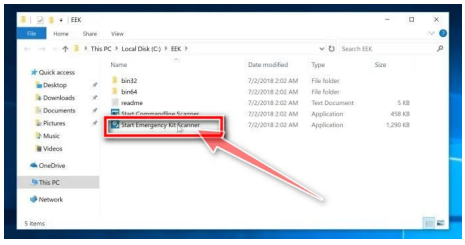
Emsisoft Emergency Kit is a free second opinion scanner that can be used without installation to scan and clean infected computers. Emsisoft scans the behavior of active files and also files in locations where malware normally resides for suspicious activity.

1. Download Emsisoft Emergency Kit.
You can download Emsisoft Emergency Kit by clicking download button.

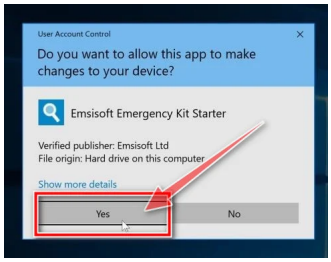
2. Install Emsisoft Emergency Kit.
Double-click on the EmsisoftEmergencyKit setup file to start the installation process, then click on the "Install" button.



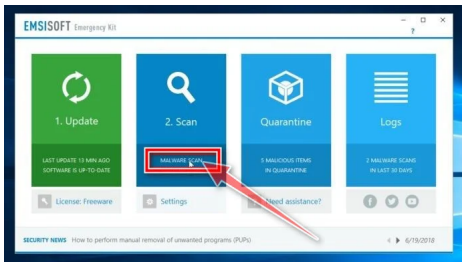
3. Start Emsisoft Emergency Kit.
On your desktop, the "EEK" folder (C:\EEK) should now be open. To start Emsisoft, click on the "Start Emsisoft Emergency Kit" file to open this program.



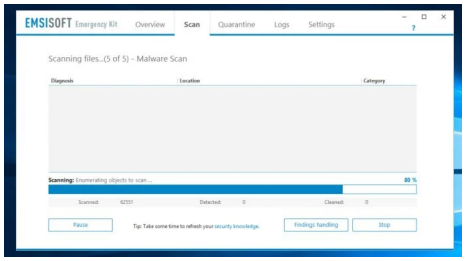
You may be presented with a User Account Control dialog asking you if you want to run this file. If this happens, you should click "Yes" to continue with the installation.



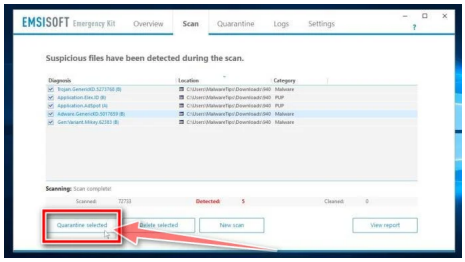
4. Click on "Malware Scan".
Emsisoft Emergency Kit will start and it will ask you for permission to update itself. Once the update process is complete, click on the "Scan" tab, and perform a "Malware Scan".



Emsisoft Emergency Kit will now scan your computer for the RRBB malicious files. This process can take a few minutes.



5. Click on “Quarantine Selected”.
When the Emsisoft scan has finished, you will be presented with a screen reporting which malicious files were detected on your computer. To remove the RRBB ransomware, click on the “Quarantine Selected“.



When the malware removal process is complete, Emsisoft Emergency Kit may need to restart your computer. Click on the “Restart” button to restart your computer.
When the process is complete, you can close Emsisoft and continue with the rest of the instructions.

STEP 5: Restore the files encrypted by the RRBB ransomware

Unfortunately, in most cases, it’s not possible to recover the files encrypted by the RRBB ransomware because the private key which is needed to unlock the encrypted files is only available through the attackers. However, below we’ve listed two options you can use to try and recover your files.

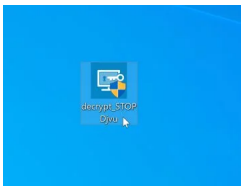
Make sure you remove the malware from your system first, otherwise, it will repeatedly lock your system or encrypt files.

Option 1: Use Emsisoft Decryptor for STOP Djvu to restore the files

If your files were encrypted with an offline key there is a chance you can recover them by using Emsisoft Decryptor for STOP Djvu decryption tool. Follow the below guide to recover your files using the Emsisoft Decryptor for STOP Djvu.

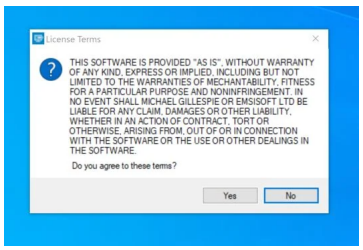
1. Download Emsisoft Decryptor for STOP Djvu
You can download Emsisoft Decryptor for STOP Djvu by clicking download button.

2. Run Emsisoft Decryptor for STOP Djvu
When Emsisoft Decryptor for STOP Djvu has finished downloading, double-click on “decrypt_STOPDjvu.exe” to run this program on your computer. In most cases, downloaded files are saved to the Downloads folder.

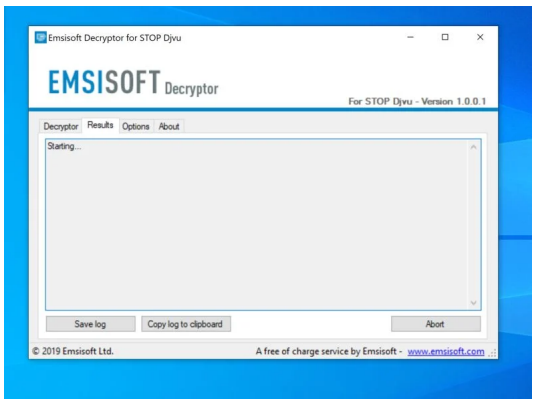


You may be presented with a User Account Control pop-up asking if you want to allow Emsisoft to make changes to your device. If this happens, you should click “Yes” to continue with the installation.

3. Follow the on-screen prompts
When the Emsisoft Decryptor for STOP Djvu starts, you will need to agree with the Terms and accept a disclaimer.



4. Click on “Decrypt”.
Click the “Decrypt” button to start the decryption process. The screen will switch to a status view, informing you about the current process and decryption status of your files.



5. The decryptor will inform you once the decryption process is finished. If you require the report for your records, you can save it by clicking the “Save log” button. If your system was compromised through the Windows Remote Desktop feature, we also recommend changing all passwords of all users that are allowed to login remotely and checking the local user accounts for additional accounts the attacker might have added.

If the “Emsisoft Decryptor for STOP Djvu” can’t decrypt your documents and you do not plan on paying the ransom, it is advised that you make an image of the encrypted drives so that you can decrypt them in the future.

Option 2: Search for a RRBB ransomware decryption tool
The cybersecurity community is constantly working to create ransomware decryption tools, so you can try to search these sites for updates:

https://id-ransomware.malwarehunterteam.com/
https://decrypter.emsisoft.com/
https://noransom.kaspersky.com/
https://www.avast.com/ransomware-decryption-tools

Your computer should now be free of the RRBB ransomware infection. If your current antivirus allowed this malicious program on your computer, you may want to consider purchasing the full-featured version of Malwarebytes Anti-Malware to protect against these types of threats in the future.