HACKER COMBAT
COMMUNITY

Ransomware - What Is It

And How To Remove It

Hackercombat.com

HACKER COMBAT COMMUNITY

What Is Ransomware?

Ransom malware, or ransomware, is a type of malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access.

The earliest variants of ransomware were developed in the late 1980s, and payment was to be sent via snail mail. Today, ransomware authors order that payment be sent via cryptocurrency or credit card.

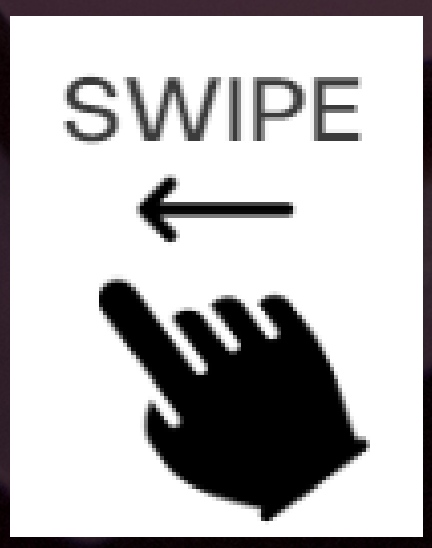
HACKER COMBAT
COMMUNITY

Ransomware is a dreaded malware that can make you lose access to your important files and photos.

Be it an individual or a business; none is entirely immune to this malicious software. This malware can lock you out of your system and demand ransom to give access back.

With cyber thieves becoming more and more sophisticated, it has become quite challenging to decrypt your files.

Hackercombat.com



HACKER COMBAT COMMUNITY

How To Remove Ransomware?

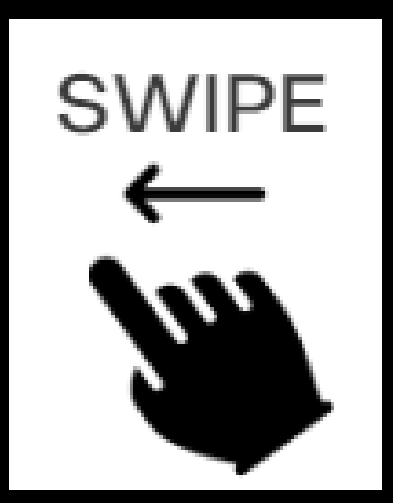
Isolate Infected Devices

Identify the Kind of Ransomware Attack

Eliminate Ransomware

Recover the Encrypted Files

Hackercombat.com



Step 1: Isolate Infected Devices

If you see phrases like ‘pay ransom’ or ‘access denied’ on your system, you have been under a ransomware attack.

If this is the case, detach all the infected wireless and wired devices and desktops.Disconnecting your devices will stop this malware from spreading and infecting more of your devices.

Make sure you disconnect the following devices:

- External hard drives
- Unshared or shared network drives
- Cloud storage accounts
- Flash drives

Further, you need to check if any of these devices were connected with the infected device. If yes, you need to check them as well for ransom messages.

Step 2: Identify The Kind Of Ransomware Attack

The next action would be to categorize the kind of ransomware that attacked your system. There are three common types of ransomware:

Locker Ransomware: Locker ransomware locks the screen of your PC and prevents you from entering the system. This type doesn't encrypt your files but denies access to your system. It will lock the GUI of your device and demands a ransom fee in exchange for the device accessibility.

Crypto Ransomware: This type of ransomware denies access to the files. Since it has an advanced encryption weapon, it isn't easy to deal with this ransomware. When it enters your device, it silently identifies the important data and encrypts it. Also, this ransomware includes a time limit.

Scare Ware Ransomware: This type of ransomware is the easiest to delete. You will see this ransomware as a fake antivirus or popups that appear on your careen on visiting an uncompromised site. This malware will tempt you to click on the popup, and once you do, it will make you download a file, which will further steal or encrypt your data.

Step 3: Eliminate Ransomware

Once you have recognized the type of malware, the next step would be to eliminate the malicious software. You can remove the malware using the following steps:

Automatic Delete: Sometimes, the ransomware gets deleted automatically after encrypting your important data. Cyber thieves don't want their ransomware to leave any clues behind that could help create decryption tools. In this case, the ransomware can be detected using security software.

Remove the ransomware with antivirus: If malware software is still on your computer, you can delete it using security software or antivirus. The same software will keep you protected from cyberattacks in the future.

Step 4: Recover The Encrypted Files

Next, you would like to recover the encrypted files. This can be done in two ways.

Restore Backed-Up Files:

It is one of the main preventive measures which marginalize the loss of data removal by ransomware.

If you've followed basic preventive measures, then you should have data backups to cloud storage or to an external device, so now is the time to recover these clean, ransomware-free files on your computer.

Automatic backup makes it easy to revert to files and software without malware.But if you haven't created a backup for your files, then, unfortunately, removing the malware and recovering it will be difficult.

Use Ransomware Decrypter:

The main objective of getting rid of a ransomware attack is to access your locked files without paying for the ransom.If cyber attackers encrypt your crucial files, find a ransomware decryption tool to decrypt or unlock your files and regain access.

Do not keep high hopes, but in rarity, you can decrypt your files without the attackers paying the ransom.

Conclusion:

Ransomware attacks are quite common these days. But, with advanced technology, it has become really difficult to outgrow the skills of hackers and cybercriminals.

So, if the above methods don't work for decrypting your important data, you can always seek professional help in the development of a custom decrypter key. If not, make sure to avoid being a victim of ransomware attacks.