

Forum:[Hack Forums](#)

Thread: [How to remove Ransomware\(try this before posting a help thread\)](#)

bulby13 - October 12, 2013, 8:09 am

Ransomware. It's big and bad. This guide will teach you how to remove the ransomware.

Names for the Ransomware type of malware

"FBI Money Pak Virus"

"DoJ virus"

Note: System restore points are not an option, ransomware can easily infect them

Instructions

1. Restart your PC by holding the power button until turned off and turning it on.

2. Press F8 repeatedly (Every 1/2 second)

3. Select Safe Mode with Networking with the arrow keys.

4. If said ransomware is still on a bit being in Safe Mode, skip to Method 2/3.

5. Download these tools:

Malwarebytes Anti-Malware(<http://www.malwarebytes.org>)

HitmanPro(<http://surfright.nl>)

TDSSKiller(<http://www.bleepingcomputer.com/download/tdsskiller/>)

Farbar Recovery Scan Tool(<http://www.bleepingcomputer.com/download/farbar-recovery-scan-tool/>)

)

Scan with these tools.

6. Reboot the machine (If Boot Menu pops up, there's an option that starts Windows normally.)

7. Do 1 more scan with each tool, to make sure.

Method 2

You will need a second computer (borrow one if you don't have one) for Methods 2 and 3

Download HitmanPro with Kickstart.

Follow these videos.

<https://www.youtube.com/watch?v=aBS902Qr0oc>

<https://www.youtube.com/watch?v=IUNHidkYsDQ>

Scan with the tools with Method 1 after.

Method 3

Download Kaspersky Rescue Disk.

Install it to an empty USB.

Plug the USB into the ransomed computer.

Access the BIOS.

Boot from USB drive (Boot -> USB drive name)

Follow prompts.

Go to terminal and type WindowsUnlocker.

After the scan, unplug and reboot.

Scan with the tools from Method 1 after.

If above methods fail

Use another boot disk, Take it to your local repair shop, or if you don't care/have a backup, you can format the drive and reinstall Windows (Last resort, or if you have those encrypter ransomware that actually encrypts your files)

Please give constructive criticism, thanks!

Note: I am not responsible for any damage to your PC. Use these tools at your own risk and

download from only trusted sources. It is always recommended to have a backup of your files

Glassy - October 13, 2013, 3:45 am

Thanks for the input of creating this guide, it will be useful. Although, I'd suggest users to first look at the [Self Help Guide's for Malware Removal](#) and use the source provided: [Removal instructions for Trojan Ransom.NoExe](#)

bulby13 - October 13, 2013, 9:31 pm

(Oct 13, 2013 03:45 AM)Glassy Wrote: [\[CITE\]](#) Thanks for the input of creating this guide, it will be useful. Although, I'd suggest users to first look at the [Self Help Guide's for Malware Removal](#) and use the source provided: [Removal instructions for Trojan Ransom.NoExe](#)

Thanks for the feedback!

To users: Tell me if you are having trouble with removal.

Automatic Coding - October 13, 2013, 9:35 pm

Any decent ransomware would have already encrypted your files/operating system before asking for a payment, so, unless you're running ransom ware made in VB.net by a twelve year old, this tutorial is somewhat useless.

However, I guess this is useful as I'm sure most ransom-ware is made in VB.net by twelve year olds now-er-days, I remember the good old days of DOS where it'd wipe your MBR and save a copy in RAM, and, only replace it if you played a game of poker and won.

Remote Administration - October 14, 2013, 5:40 am

Nice! Thanks for this, this can help with so many things!

bulby13 - October 14, 2013, 7:58 am

Thanks for all the feedback!

@Automatic Coding:

You're right, most ransomware are poorly coded by 12 year olds nowadays. I bet the encrypter ransomwares are just some stolen encrypter or c/p, although they make skids think their cool.

Muudea - October 14, 2013, 8:58 am

Thank you for posting this. It helps a bunch!

Automatic Coding - October 14, 2013, 3:19 pm

(Oct 14, 2013 07:58 AM)bulby13 Wrote: [\[CITE\]](#) Thanks for all the feedback!

@Automatic Coding:

You're right, most ransomware are poorly coded by 12 year olds nowadays. I bet the encrypter ransomwares are just some stolen encrypter or c/p, although they make skids think their cool.

I never understand people who say "Omg copyandpaste code noob", programming is very copy-and-paste based. Libraries are made for making it easier to copy and paste, same with objects, libraries, functions, and, overloading.

It's fucking stupid to say "Omg copy and paste n00b."

Groseph_Dirt - October 14, 2013, 4:48 pm

Ransomware differs depending on a lot of things.

This method would not work if you for example happen to contract a ransomware/rogueware utilizing a zeroaccess rootkit that rewrites your mbr and hides itself well. In which case running those without supervision may result in a worse infection.

