

Forum:[Hack Forums](#)

Thread: [How to Remove a basic Ransomware](#)

Blood_Hawk - June 10, 2014, 3:46 pm

How to remove a basic Ransomware virus on your Computer

I will providing multiple methods since there are multiple ways of doing this.

Method 1

1. Shutdown your Computer
2. Hit F8 when your computer is starting up, or access Safemode in any way your operating system supports.
3. Choose Safemode or Safemod with Networking
4. When the desktop appears then you know Safemode works, however, if safemode doesn't work then it's because the virus deleted a file essential to running in Safemode, skip this method.
5. However if Safemode does work, continue following the steps.
6. Open Task Manager, go to the start-up option and find the virus name and then disable the virus from running again on next re-boot. Or you can find the virus location and delete it from there.
7. When the virus is disabled then re-boot and then you should be all fine.

Method 2

1. Start your browser then access your browsing source and type in "procexp" and download it.
2. Run procexp while virus is running, however, if the virus blocks this then this method doesn't work for you.
3. When procexp is open then find the virus and kill it.
4. Usually viruses doesn't block this process.

Usually one of these 2 methods should work for the basic ransomware viruses.

we r num 1 - June 10, 2014, 3:48 pm

You need to post sources because this was obviously stolen.

UnOriginalUsername - June 10, 2014, 3:49 pm

Nice tutorial I guess but most ransomawre these days are a bit harder to get rid off.

Usually the ransomware I test can be removed from safe mode.

Blood_Hawk - June 10, 2014, 3:49 pm

(Jun 10, 2014 03:48 PM)Wzards Wrote: [\[CITE\]](#) You need to post sources because this was obviously stolen.

Dafuq? How? I've had experience with ransomware. I didn't steal this..

Aura - June 10, 2014, 3:53 pm

Quote:Method 2

1. Start your browser then access your browsing source and type in "procexp" and download it.
2. Run procexp while virus is running, however, if the virus blocks this then this method doesn't work for you.
3. When procexp is open then find the virus and kill it.
4. Usually viruses doesn't block this process.

Are you dumb if you're infected with a Ransomware you won't even have access to a web browser ... do you know what a ransomware is ?

Vanilja - June 10, 2014, 3:53 pm

So what if the ransomware blocks safe mode?

we r num 1 - June 10, 2014, 3:54 pm

(Jun 10, 2014 03:53 PM)Aur? Wrote: [\[CITE\]](#) Are you dumb if you're infected with a Ransomware you won't even have access to a web browser ... do you know what a ransomware is ?
Exactly yet he has experience with it...

I could have better methods to counter ransomware with only my little knowledge in malware.

Quest™ - June 10, 2014, 3:54 pm

He's just trying to be helpful don't bash him. Just teach him what he doesn't know.

Aura - June 10, 2014, 3:55 pm

(Jun 10, 2014 03:54 PM)Google Hangouts Wrote: [\[CITE\]](#) He's just trying to be helpful don't bash him. Just teach him what he doesn't know.

When you don't know what you're talking about, you don't post "tutorials". It's just false information and you're doing more harm than good.

Null Byte - June 10, 2014, 3:56 pm

Uh, just so you know task manager doesn't list all persistence locations. You could have a hijacked system file in which case you'd have to use a hash check to find it. Also, if it's installed as a driver, you're fucked with the first method too. Now lets look at the second method. What makes you think you'll have access to a web browser that can download files? That's a huge, inaccurate assumption.

This guide really needs some work.

Quest™ - June 10, 2014, 3:56 pm

(Jun 10, 2014 03:55 PM)Aur? Wrote: [\[CITE\]](#) When you don't know what you're talking about, you don't post "tutorials". It's just false information and you're doing more harm than good.
Very true that's why I don't post tutorials.

Blood_Hawk - June 10, 2014, 3:57 pm

(Jun 10, 2014 03:53 PM)Saixen-© Wrote: [\[CITE\]](#) So what if the ransomware blocks safe mode?
It says "Basic Ransomware", the ransomware would have to delete a file that is essential to run in safemode, i guess most basic ransomware wouldn't do that. However if so, then you would have to restore windows and have a file backup service with your files.

Null Byte - June 10, 2014, 3:57 pm

(Jun 10, 2014 03:54 PM)Google Hangouts Wrote: [\[CITE\]](#) He's just trying to be helpful don't bash him. Just teach him what he doesn't know.

What's worse then not helping someone? "Helping" them with false information. He's just wasting their time.

Aura - June 10, 2014, 3:58 pm

(Jun 10, 2014 03:57 PM)Blood_Hawk Wrote: [\[CITE\]](#) It says "Basic Ransomware", the ransomware would have to delete a file that is essential to run in safemode, i guess most basic ransomware wouldn't do that.

Once again you're dumb.

Even "basic" ransomwares block access to your web browser so solution 2 is useless.

Null Byte - June 10, 2014, 3:59 pm

OP I think it would be in your best interest to close the thread. You're really lucky Corso isn't here or else you'd probably be crying in the shower right now.

Blood_Hawk - June 10, 2014, 4:00 pm

(Jun 10, 2014 03:53 PM)Aur? Wrote: [\[CITE\]](#) Are you dumb if you're infected with a Ransomware you won't even have access to a web browser ... do you know what a ransomware is ?

.- Are you serious? Look up ransomware, of course you would have access to a web browser..

Aura - June 10, 2014, 4:01 pm

(Jun 10, 2014 04:00 PM)Blood_Hawk Wrote: [\[CITE\]](#) -.- Are you serious? Look up ransomware, of course you would have access to a web browser..

... You're a fucking idiot.

A RANSOMWARE LOCKS DOWN YOUR WHOLE COMPUTER, YOU DON'T HAVE ACCESS TO ANYTHING.

YOU'RE TALKING ABOUT A SCAMWARE, NOT A RANSOMWARE IDIOT.

T e s s e r a c t - June 10, 2014, 4:01 pm

In a perfect world where Ransomware knocks at your door to tell you Safe Mode is available, whoops was it story time? I could have sworn thats what the topic was.

No OP. Ransomware can get sticky as I like to call it, and infect boot sectors and even the MBR, then you have to flash your BIOS and a whole bunch of junk.

But lets be honest, we would all try out Safe Mode before being a complete idiot and attempting something delirious i.e. flashing the BIOS first or reformatting in a worse case scenario.

The best thing to do if the Ransomware does not encrypt your files is to boot into a Linux distro such as Mint and simply extract important files from the user profile's directory. Take a screenshot of software used on the machine before. Then begin a diagnosis.

[img]<http://media.giphy.com/media/nnFYOiVQ7qHNm/giphy.gif>[/img] Sometimes how I feel.

Vanilja - June 10, 2014, 4:02 pm

(Jun 10, 2014 03:57 PM)Blood_Hawk Wrote: [\[CITE\]](#) It says "Basic Ransomware", the ransomware would have to delete a file that is essential to run in safemode, i guess most basic ransomware wouldn't do that. However if so, then you would have to restore windows and have a file backup service with your files.Or you could just to boot up from live cd, like hiren or kaspersky and edit the registry a little and delete few files.

Null Byte - June 10, 2014, 4:02 pm

(Jun 10, 2014 04:00 PM)Blood_Hawk Wrote: [\[CITE\]](#) -.- Are you serious? Look up ransomware, of course you would have access to a web browser..

I don't see a webbrowser anywhere

<http://spyware-removal-guide.net/images/FBI-moneypack-US-2.jpg>

Blood_Hawk - June 10, 2014, 4:02 pm

(Jun 10, 2014 03:58 PM)Aur? Wrote: [\[CITE\]](#) Once again you're dumb.

Even "basic" ransomwares block access to your web browser so solution 2 is useless.

Facepalm... Look it up... How fucking stupid can someone be..

Aura - June 10, 2014, 4:03 pm

This thread is done.

OP is so dumb he doesn't know the difference between a scamware and a ransomware.

Null Byte - June 10, 2014, 4:03 pm

(Jun 10, 2014 04:02 PM)Saixen-© Wrote: [\[CITE\]](#) Or you could just to boot up from live cd, like hiren or kaspersky and edit the registry a little and delete few files.

THIS is the proper way to remove ransomware. The procedure recommended in the thread is egregiously false.

Aura - June 10, 2014, 4:03 pm

(Jun 10, 2014 04:02 PM)Blood_Hawk Wrote: [\[CITE\]](#) Facepalm... Look it up... How fucking stupid can someone be..

You are fucking stupid idiot.

You're talking about a SCAMWARE, not a RANSOMWARE. CryptoLocker IS a Ransomware, do you have access to a web browser ? NO IDIOT.

Quest™ - June 10, 2014, 4:03 pm

How to Remove a basic Ransomware

Navigate to: <http://www.bleepingcomputer.com/virus-removal/>

And find the name of the ransomware.

desynk - June 10, 2014, 4:05 pm

I don't like this guide. You make it sound like removing malware comes down to just a few easy steps, it's not like that in reality. Also killing a process off usually (99.999999%) does not kill a virus.

Blood_Hawk - June 10, 2014, 4:07 pm

(Jun 10, 2014 04:01 PM)Aur? Wrote: [\[CITE\]](#) ... You're a fucking idiot.

A RANSOMWARE LOCKS DOWN YOUR WHOLE COMPUTER, YOU DON'T HAVE ACCESS TO ANYTHING.

YOU'RE TALKING ABOUT A SCAMWARE, NOT A RANSOMWARE IDIOT.

Holy shit... A ransomware locks your computer until you pay a certain amount of money, god...

Vanilja - June 10, 2014, 4:08 pm

(Jun 10, 2014 04:00 PM)Blood_Hawk Wrote: [\[CITE\]](#) -.- Are you serious? Look up ransomware, of course you would have access to a web browser..Wait what?

Do you even know what a ransomware is?

I guess you copied this whole post from somewhere, fail.

Not sure how you gonna access web browser if this pops up on your screen

<http://cdn.arstechnica.net/wp-content/uploads/2013/10/MoneyBank.jpg>

Aura - June 10, 2014, 4:09 pm

(Jun 10, 2014 04:07 PM)Blood_Hawk Wrote: [\[CITE\]](#) Holy shit... A ransomware locks your computer until you pay a certain amount of money, god...

You just made yourself loose that argument. "A ransomware locks your computer until you pay a certain amount of money" (DUH DUMBASS). Now tell me HOW you're going to access a web browser when that ransomware is LOCKING DOWN your computer ?

Fucking GG idiot, you just lost so hard and you fucked up.

Blood_Hawk - June 10, 2014, 4:11 pm

(Jun 10, 2014 04:09 PM)Aur? Wrote: [\[CITE\]](#) You just made yourself loose that argument. "A ransomware locks your computer until you pay a certain amount of money" (DUH DUMBASS). Now

tell me HOW you're going to access a web browser when that ransomware is LOCKING DOWN your computer ?

Fucking GG idiot, you just lost so hard and you fucked up.

-.-, ok, what do you think, use common sense here.. Just come on here, just try..

cyberducky - June 10, 2014, 4:11 pm

(Jun 10, 2014 04:09 PM)Aur? Wrote: [\[CITE\]](#) You just made yourself loose that argument. "A ransomware locks your computer until you pay a certain amount of money" (DUH DUMBASS). Now tell me HOW you're going to access a web browser when that ransomware is LOCKING DOWN your computer ?

Fucking GG idiot, you just lost so hard and you fucked up.

LOL I know Aura I read this and was like what? OP don't post tutorials on shit you don't know.

Aura - June 10, 2014, 4:12 pm

(Jun 10, 2014 04:11 PM)Blood_Hawk Wrote: [\[CITE\]](#) -.-, ok, what do you think, use common sense here.. Just come on here, just try..

Okay I'm done.

You're obviously a troll. You just contradicted yourself yet you think you're still right ?

Requesting this thread to be closed.

Blood_Hawk - June 10, 2014, 4:13 pm

(Jun 10, 2014 04:12 PM)Aur? Wrote: [\[CITE\]](#) Okay I'm done.

You're obviously a troll. You just contradicted yourself yet you think you're still right ?

Requesting this thread to be closed.

Took you some time to fucking figure that out didn't it?

Quest™ - June 10, 2014, 4:13 pm

Well OP wasted money on L33T gg skid

-Hyperion - June 10, 2014, 4:14 pm

(Jun 10, 2014 04:11 PM)Blood_Hawk Wrote: [\[CITE\]](#) -.-, ok, what do you think, use common sense here.. Just come on here, just try..

By booting into safe mode? Sorry most ransomware will still load even if you could get to safe mode. The best solution would be to run HitmanPro Kickstart. Also on behalf of Canada I apologize for Auru's language.

Aura - June 10, 2014, 4:14 pm

(Jun 10, 2014 04:13 PM)Blood_Hawk Wrote: [\[CITE\]](#) Took you some time to fucking figure that out didn't it?

No I knew it from the start but I needed to rant after sending my days proving dumbasses like you wrong.

we r num 1 - June 10, 2014, 4:14 pm

Now he is going to play the "I was trolling the whole time" card so he doesn't feel like an idiot. LMFAO HOLY SHIT...