

Forum:[Hack Forums](#)

Thread: [How to remove Auto screen lock virus &\[b\]#34\[/b\]; Metropolitan police virus&\[b\]#34\[/b\];](#)

Contracting - October 11, 2013, 1:34 pm

So, This is a virus where the hackers Lock your desktop screen and tell you to pay to unlock it, Yes if you pay it will be unlocked, But its a scam and a hack so if you do pay cancel your credit card immediately. So lets get started.

Do not pay what so ever! You are being drawn in to their trap!

1. Restart computer with safe mode.
2. Once on your computer go to control panel.
3. Find system restore.
4. Select system restore and restore it to a few days back for e.g you got the virus on the 11/10/13 (English dates) Change it back to 9/10/13 Or you can select to change it back when you last downloaded something.
5. restart your pc and it should be fine any more help pm me or leave a comment.

White hat for the win bitches!

Benjamin Franklin - October 11, 2013, 1:40 pm

Most malware now infects System Restore points. Restoring can make the infection worse.

Terror32 - October 11, 2013, 1:42 pm

And the new version of "Metropolitan police virus" shutdowns PC when you enter safe mode. Best thing is to use USB/CD boot antivirus and clean it or try to switch users it works on some versions of virus.

Contracting - October 11, 2013, 1:43 pm

(Oct 11, 2013 01:42 PM)Day Trader Wrote: [\[CITE\]](#) And the new version of "Metropolitan police virus" shutdowns PC when you enter safe mode. Best thing is to use USB/CD boot antivirus and clean it or try to switch users it works on some versions of virus.

Yeah, you could always just make a new user, or use trojan killer, Just trying to help anyway

Income. - December 10, 2013, 2:06 pm

Old thread but this may help someone.

If you got a virus that wont let you in safemode it usually works if you search MSCONFIG go in it and search through the tabs and look for Safemode then reebot.

You can also look for startups when you're in MSCONFIG and disable viruses that starts up when the power is turning on.

Good Luck.

#Thunder - December 10, 2013, 2:07 pm

(Dec 10, 2013 03:06 PM)P S N b u u s a ™ Wrote: [\[CITE\]](#) Old thread but this may help someone.

If you got a virus that wont let you in safemode it usually works if you search MSCONFIG go in it and search through the tabs and look for Safemode then reebot.

You can also look for startups when you're in MSCONFIG and disable viruses that starts up when the power is turning on.

Good Luck.

We would appreciate it if you don't grave dig threads.

#Reliant - December 10, 2013, 2:09 pm

#Thunder Wrote: [\[CITE\]](#) (Today 03:06 PM)P S N b u u s a ™ Wrote: ?Old thread but this may help someone.

If you got a virus that wont let you in safemode it usually works if you search MSCONFIG go in it and search through the tabs and look for Safemode then reebot.

You can also look for startups when you're in MSCONFIG and disable viruses that starts up when the power is turning on.

Good Luck.

We would appreciate it if you don't grave dig threads.He was providing help, and this thread isn't terribly old, but it is indeed a couple months old. In this case, it isn't all that bad.

Aura - December 10, 2013, 3:24 pm

(Dec 10, 2013 03:06 PM)P S N b u u s a ™ Wrote: [\[CITE\]](#) Old thread but this may help someone.

If you got a virus that wont let you in safemode it usually works if you search MSCONFIG go in it and search through the tabs and look for Safemode then reebot.

You can also look for startups when you're in MSCONFIG and disable viruses that starts up when the power is turning on.

Good Luck.

You're answer isn't really accurate.

There's Ransomwares/Scamwares that can hide themself from the Start-Up (meaning they were injected with a RootKit), which means that they won't show up in msconfig Start-Up list. Also, msconfig Start-Up list doesn't show every keys that are ran on either boot or session opening, which means the Ransomware/Scamware will not necessary show up in the msconfig Start-Up list.

So in summary, your "method" isn't that good as there's big chances you won't be able to disable the Ransomware/Scamware only by unchecking it via msconfig as you may not even see it in that list.

Income. - December 11, 2013, 4:45 am

(Dec 10, 2013 04:24 PM)Aur? Wrote: [\[CITE\]](#) You're answer isn't really accurate.

There's Ransomwares/Scamwares that can hide themself from the Start-Up (meaning they were injected with a RootKit), which means that they won't show up in msconfig Start-Up list. Also, msconfig Start-Up list doesn't show every keys that are ran on either boot or session opening, which means the Ransomware/Scamware will not necessary show up in the msconfig Start-Up list.

So in summary, your "method" isn't that good as there's big chances you won't be able to disable the Ransomware/Scamware only by unchecking it via msconfig as you may not even see it in that list. Yes I know that and I'm sorry that I didn't explain that I was more aiming at other malware than rootkits such as RATs etc.

As you said sir, I've only seen rootkit once in system start-up but I guess it's not usual.

Main thing I was pointing at was that it will work to get safemode back via MSCONFIG if any virus disabled it, atleast everytime I've tried.

Aura - December 11, 2013, 5:09 am

(Dec 11, 2013 05:45 AM)P S N b u u s a ™ Wrote: [\[CITE\]](#) Yes I know that and I'm sorry that I didn't explain that I was more aiming at other malware than rootkits such as RATs etc.

As you said sir, I've only seen rootkit once in system start-up but I guess it's not usual.

Main thing I was pointing at was that it will work to get safemode back via MSCONFIG if any virus disabled it, atleast everytime I've tried.

This would be for Ransomwares/Scamwares that were not injected via a RootKit so yes in a sense it could work. Now it's pretty rare to see that you can disable malwares via the msconfig, but in the past it uses to work.