

Forum:[Hack Forums](#)

Thread: [Idea to completely clean a pc and recover files will this work?](#)

JohnHolesten - December 25, 2016, 3:54 am

People these days are too worried about not wiping their pc.

I think its a stupid idea to not wipe your pc and try all these "Tools" because all you have to do is have a crappy pc you dont use and a usb and your infected computer because with these 3 things you can use to defeat someone who has infected your pc.

This is assuming your files are not crypto crap locked, ect.

1. Recover important files and store them on usb
2. Use crappy pc and go to a internet caffe with you crap lappy.
3. Scan all files from usb on Virus Total.
4. wait one month and wipe laptop.
5. Go to another internet caffe and repeat 3.
6. Because virus total sends files scanned to anti virus company's likely your files would have gone through a complex protocols and tests to discover any virus crypted out the ass and hopefully next time you scan the file either its clean or if the virus was hiding in those important files it is detected preventing your pc from being infected again.

My Question is would this idea work?

ka\$h - December 25, 2016, 3:59 am

You want someone to wait one month to check if their files are infected? people can reverse engineer, test, and analyse malware in so many other ways.

And no it won't work.

JohnHolesten - December 25, 2016, 4:07 am

(Dec 25, 2016 04:59 AM)ka\$h Wrote: [\[CITE\]](#) You want someone to wait one month to check if their files are infected? people can reverse engineer, test, and analyse malware in so many other ways.

And no it won't work.

What exact part of it wont work?

ka\$h - December 25, 2016, 4:14 am

(Dec 25, 2016 05:07 AM)JohnHolesten Wrote: [\[CITE\]](#) What exact part of it wont work?

Mainly step 6, there are just too many things wrong with it, mainly the fact that the protocols you speak of are not always capable of exposing malware or else the malware of been recognised originally when it was scanned.

You say this is a way of defeating malware in the perspective of already being infected, as in defeating it once your infected; if your infected what is scanning a file you know to be malware going to do?

And you know without step 6 the whole thing is just a waste of time and falls to pieces.

JohnHolesten - December 25, 2016, 4:20 am

(Dec 25, 2016 05:14 AM)ka\$h Wrote: [\[CITE\]](#) Mainly step 6, there are just too many things wrong with it, mainly the fact that the protocols you speak of are not always capable of exposing malware or else the malware of been recognised originally when it was scanned.

You say this is a way of defeating malware in the perspective of already being infected, as in defeating it once your infected; if your infected what is scanning a file you know to be malware going to do?

I certainly did not think of it in that perspective but im sure malware arent that 99% malware arent that smart. Maybe there is that 1% that is but im pretty sure companies would crack down on that 1% the most.

Like it was just an idea i came up with randomly and wrote it down without thinking about it.

Would there be an actual way to do the same goal successfully that is similar?

ka\$h - December 25, 2016, 4:36 am

(Dec 25, 2016 05:20 AM)JohnHolesten Wrote: [\[CITE\]](#) I certainly did not think of it in that perspective but im sure malware arent that 99% malware arent that smart. Maybe there is that 1% that is but im pretty sure companies would crack down on that 1% the most.

Like it was just an idea i came up with randomly and wrote it down without thinking about it.

Would there be an actual way to do the same goal successfully that is similar?

If your relying on a tool such as an anti-virus it'll only ever be as good as their detection techniques. The only other way I can think of which relates to analysing a file properly is through reverse engineering. If not that then there are more efficient ways to test malware such as in virtual environments.

Elitas - December 25, 2016, 4:59 am

I doubt this would work. Much easier methods.