

Forum:[Hack Forums](#)

Thread: [External Disk infected + computer potentially infected too.](#)

Kolz - October 7, 2015, 10:35 am

Hey guys, I need some help.

My father told him that his external disk wouldn't show its files yet was using 300gb, I found that weird, looking up avast & all, it showed multiple infections. I used tools such as Junkware Removal Tool etc but it did nothing, in addition the files are currently hidden, some were converted to .scr extension files etc. Unfortunately I have no clue how to proceed, nor how to actually fix to make sure his files aren't gone forever, it contains all of the files required for his school work so getting rid of them all isn't an option unfortunately. I'm not sure what exactly's infected in it so I would gladly welcome any help, thanks.

Avast scan:

Docs are hidden: (I made it show hidden files)

Anyone has a clue in what I can do? I did some quick searches but not much that would make me confidently proceed. Is USBFix a potential good solution to solve the issue or should I do anything else? Any advice or help would be appreciated asap since he'll need his school stuff.

Thanks.

Knautschtabak - October 7, 2015, 12:08 pm

Hey Kolz.

These files have likely been replaced by the malware (which means they might have been overwritten). Please take a look into the .Trashes folder. Some worms like Bondat move the files there instead of replacing them.

To be sure what kind of infection we are dealing with, please upload one of the infected files to [virustotal.com](#) and [hybrid-analysis.com](#) (place a checkmark on Win7 32 bit 'Stealthy Mode'). Make sure to choose a file that is not confidential in case that parts of the original file are still there. Post the links to the uploads here.

After that I will be able to give you more information regarding the status of your father's files.

Furthermore, the machine of your father and any other system that was connected to the external drive is likely infected. Do NOT double-click on any of those files, this will run the malware.

Do NOT connect the infected external drive to a non-infected machine.

Other removable devices (USB sticks etc) that have been connected to your father's machine lately are likely infected too. Do NOT connect them to other machines.

In short: Handle everything that had direct or indirect contact to the infected machine as probably infected.

Kolz - October 7, 2015, 12:29 pm

(Oct 7, 2015 12:08 PM)Knautschtabak Wrote: [\[CITE\]](#) Hey Kolz.

These files have likely been replaced by the malware (which means they might have been overwritten). Please take a look into the .Trashes folder. Some worms like Bondat move the files there instead of replacing them.

To be sure what kind of infection we are dealing with, please upload one of the infected files to virustotal.com and hybrid-analysis.com (place a checkmark on Win7 32 bit 'Stealthy Mode'). Make sure to choose a file that is not confidential in case that parts of the original file are still there. Post the links to the uploads here.

After that I will be able to give you more information regarding the status of your father's files.

Furthermore, the machine of your father and any other system that was connected to the external drive is likely infected. Do NOT click on any of those files, this will run the malware.

Do NOT connect the infected external drive to a non-infected machine.

Other removable devices (USB sticks etc) that have been connected to your father's machine lately are likely infected too. Do NOT connect them to other machines.

The .trashes folder seem to only have torrented movies etc apparently. Some files do indeed appear to have been overwritten and no longer work at all, in addition they appear to only be 1kb at most now (I tried before I got the advice not to open them, whoops.) :/.

Not really sure how I'm supposed to know which files are infected, Avast seems to still have them on quarantine, however here's Virustotal of a file that doesn't seem to work and probably got overwritten:

<https://www.virustotal.com/en/file/83f9dca6ef2bc179eddb6166c9424d64d62c4ed7271975544569a2d31b0f0b63/analysis/1444245795/>

Everytime I try it on hybrid analysis, it fails with "raw data" can't be read or some message like this ("The file format "raw data" is not supported"). edit: hasn't worked with multiple kind of files. Not sure what to do about it.

Thanks for the help by the way.

Knautschtabak - October 8, 2015, 3:31 am

Hi Kolz.

The file that you send to VT is corrupt.

If you just rename the .doc extension to .txt and open it in a text editor, you will see something like:

Code ELAJMI

ELAJMI MingLiU SimSu

n ~@ ÿÿÿÿ 9w

Avast did not quarantine that specific file, because it is corrupt.

I need a sample from the Avast Virus Chest.

Please look at the following article:

<https://blog.avast.com/2013/11/03/how-do-i-access-the-avast-virus-chest/>

The video there tells you how to access the quarantined files. Please restore one or two of them and send them either to me (with a fileupload service) or to hybrid-analysis.com (they will share the sample so I can download it too). Send me the link.

hybrid-analysis did complain previously, because the file cannot be executed.