



How to remove malware from an infected windows PC

This is a guide to demonstrate how to detect and remove malware viruses from infected windows PCs.

Written By: George A.

An advertisement for Malwarebytes 3.0. The background is a dark blue cityscape at night with a large, mechanical, tentacle-like creature on the right. The text 'MALWAREBYTES 3.0: NOW STRONGER AND SMARTER' is at the top left. The main title 'MAKES ANTIVIRUS OBSOLETE' is in large, white, sans-serif capital letters. Below it, smaller text reads 'Four layers of malware-crushing tech. Smarter detection. Specialized ransomware protection. It's the security you've been looking for.' At the bottom left are two buttons: 'FREE DOWNLOAD' in a grey box with a red border and 'BUY NOW' in a blue box. A link 'What's the difference?' is also present.

This document was generated on 2019-09-17 10:14:21 AM (MST).

INTRODUCTION

You will need to have a second windows PC if the infected PC does not boot.

TOOLS:

- SATA to USB adapter or open SATA port inside PC. (1)

Step 1 — Install Anti-Malware software



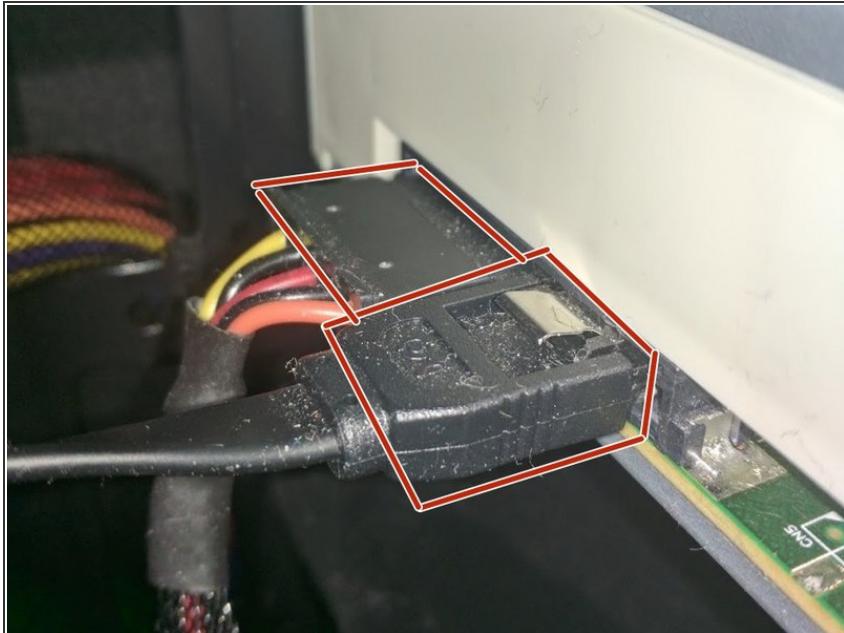
- On the PC you will be doing antivirus on, install the appropriate software. If the PC with malware does not turn on, install on a different one to do anti-virus.
- Malwarebytes is great anti-virus software. Go to the [website](#) and install it for free.
- Glarysoft Malware hunter is also good. Their website is [here](#).
- *(i)* Other free anti-malware works too, but these are my favorites.

Step 2 — Remove your SATA HDD/SDD from the PC



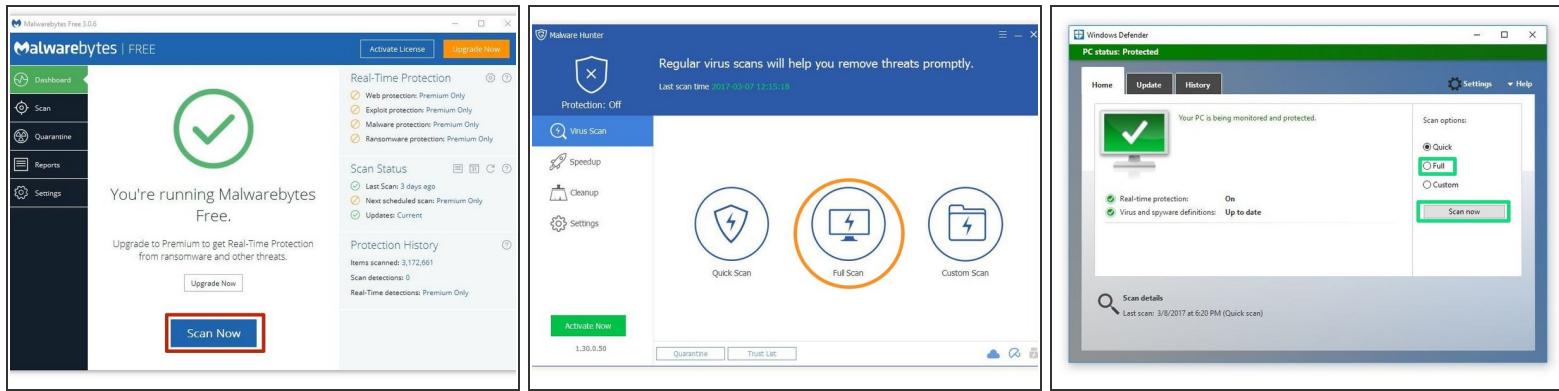
- ☒ This step only applies to PCs that do not boot. If the PC with malware runs, then install the software directly onto it.
- Because assembly of different laptops and PCs vary so much, you will have to figure out or find a guide to remove your drive.

Step 3 — Connect the drive



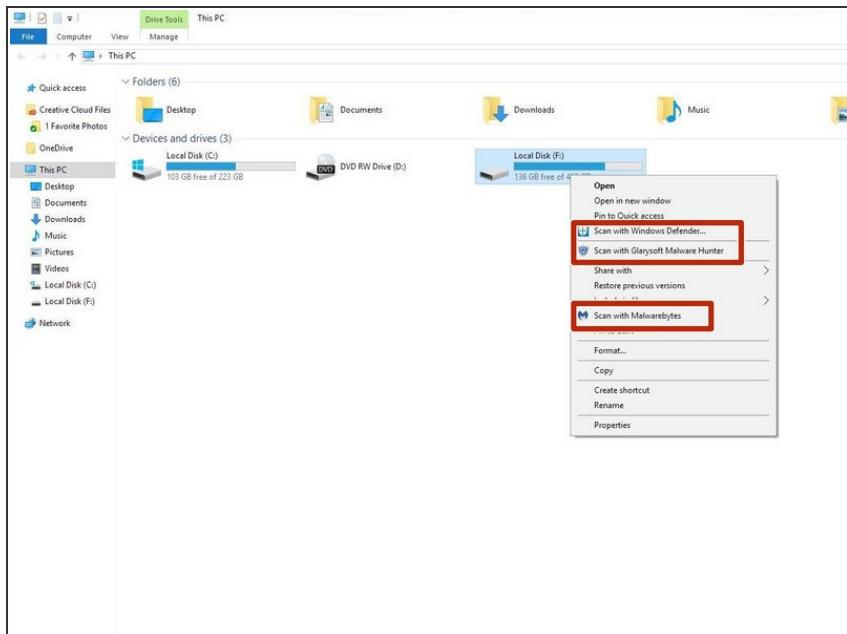
- ☒ This step also only applies to PCs that don't boot.
- If your non-infected PC is a desktop, you may unplug the optical drive and plug the connections into the HDD or SSD. If it is a laptop, you will need a [SATA to USB adapter](#).
- ⓘ Shut down your desktop before unplugging the DVD drive and attaching the HDD.

Step 4 — Disinfect your PC



- Once you've installed the necessary programs and (if applicable) connected you're infected drive to you PC, you are ready to be the doctor.
- Run Malwarebytes.
- Run Glarysoft Malware Hunter.
- Windows defender comes preinstalled with Windows. Use that also.

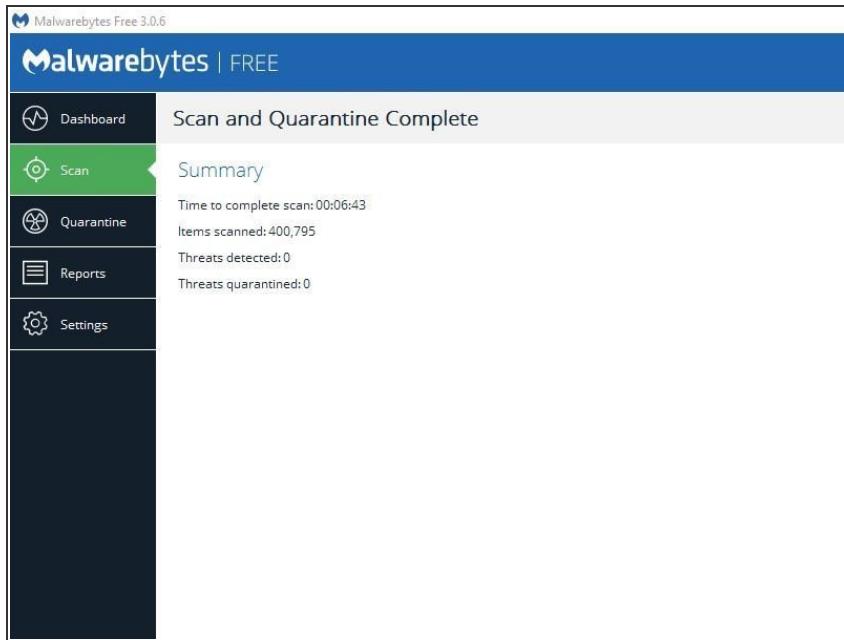
Step 5 — Double checking another PCs drive.



→ This is the last step for checking another PCs drive

- Go into file explorer, right click on the drive from the infected PC, and select each of the highlighted options.

Step 6 — Finito!



- All done! follow these instructions in reverse to put everything back.