Malware Removal Guide

If you suspect you are infected with Crypto malware or your computer DOES NOT successfully boot DO NOT follow this guide!

What is malware?
Malware is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software. [Source: Wikipedia.com]

How did I get infected?
It is difficult to track down the source of an infection. Most infections are given permission to run unknowingly by the user. It is recommended to keep User Account Control turned on and never give access to something you do not trust or did not open. Many other infections come from exploits in your browser or browser plug-ins on sites you visit. When your downloading programs, always use the publisher's website directly.

Purpose of this Guide

This guide was created to help the average user in removing malware from an infected system that boots into windows, meaning you can successfully login and navigate to the desktop. Following this guide step by step will result in successfully malware removal 90% of the time. That said, there's still the 10% percent that exists that this guide will not remove such as Crypto malware that locks your data behind a paywall. The tools recommended in this guide were picked because they have high success and low failure rates. I am writing this guide in layman's terms so that most people will be able to understand it with ease.

Disclaimer

The following tools and software are by recommendation only, it is solely YOUR responsibility to save all work and back up any and all important data on your system before proceeding. Even with countless successful attempts using the methods described below there is still a possibility of failure.

Malware Removal Steps
1) Run rkill.com (1). Sometimes it takes a few minutes to finish. Do not reboot when done.
Short Description Kills malware processes, Removes policies in the registry that would prevent normal windows operation, Repairs file extension hijacks.

2) Download an updated copy Malwarebytes 3.0 (2). Turn on the "Scan for Rootkits" option. Then, run a "Scan"
Short Description Successfully removes the vast majority of infections, Has built-in rootkit/bootkit scanning engine, Has built-in repair tools to fix damage done by malware.

3) Run Malwarebytes ADWCleaner (3) using the "Scan" option. Then click "Cleaning" when its finished and allow it to reboot your system.
Short Description Removes majority of adware, PuPs, Toolbars, and Browser hijacks, Fixes proxy settings changed by malware, Removes certain non-default browser settings.

4) Run Malwarebytes Junkware Removal Tool (4) and allow it to finish. Reboot your computer upon completion.
Short Description Removes adware, PuPs, Toolbars, and Browser hijacks other tools miss, Good at removing unneeded AppData directories left behind by infections

Network Repair If malware has blocked you from browsing the web, you can try to run the NetAdapter Repair Tool (5) with 'all options checked' which will try to restore your internet connection and restore your browser. You will most likely have to download these tools on another computer and move them to a flash drive that you can plug into the infected machine.

Have adware or spyware on your Mac?
Try Malwarebytes Anti-Malware for Mac (formerly Adware Medic) (6).

Follow-up Steps (highly recommended):

- Using a computer that has not been infected, change passwords to all your online accounts.
- Consider enabling two-factor authentication.

How to prevent future infections:
Be very careful what you download and install. Keep programs like Java & Flash up-to-date, but do so using their official websites or using the website Ninite (7), it packages software together for a faster install. Use Unchecky (8) to automatically uncheck software suggestions and prevent accidental installation of adware & spyware during product installations. Make sure Windows is kept up-to-date as well. The first line of defense starts with you.

The following tools will aide you in keeping your computer clean:

Downloads to mentioned tools/software
1 https://www.bleepingcomputer.com/download/rkill/dl/132/
2 https://downloads.malwarebytes.org/file/mbam_current
3 https://toolslib.net/downloads/viewdownload/1-adwcleaner/
4 http://www.bleepingcomputer.com/download/junkware-removal-tool/)
5 http://www.bleepingcomputer.com/download/netadapter-repair-all-in-one/
6 https://www.malwarebytes.org/mac-download/
7 https://ninite.com/
8 http://unchecky.com