Malware Guide

Purpose & Scope of this Guide:

This guide is designed to inform you of the best ways to remove malware from your computer, and how to best protect yourself from malware in the future. Not all malware is created equal, even the best protection and most knowledgeable users will get malware eventually. There is no one way to never get malware, being online adds malware risk.

Malware remediation steps

If your files are encrypted, do not follow any steps in this guide until you read this article on ransomware.

The only way to guarantee all malware is removed from your system is to do a clean install. The anti-malware tools listed below can only take their best shot at removing malware from your system. There is no guarantee that any tools, listed in this guide or not, will remove all malware from your system. AV/AM tools can only think your system doesn't have malware.

If you would like to attempt to remove malware from your system, you can run the three tools listed below.

1. RKill
2. Malwarebytes ADW cleaner
3. Hitman pro

How to protect yourself in the future

- Make sure you are using non-EOL software & OS. Operating systems like Windows XP, Vista, and 7 carry additional security risks as they are no longer being supported by Microsoft. Running pre-release, beta, insider, or preview builds can also carry additional risks.
- Make sure you are updating your software & OS. Updates often include security patches, which malware can exploit if left unpatched.
- Make sure you are running an anti-virus. Windows includes Windows Defender by default, and that is all most people need. See here for our stance on paid AVs. If you don't like Windows Defender, running an AV is better than running none.
- For protection against ransomware, make sure you keep good backups of your data. Backups are preemptive, not reactive. You cannot backup your data after it is lost.
- Running an adblocker like ublock origin is a great way to protect yourself online. Malicious

advertisements exist and are a fairly common way to get malware in the first place. You can find download links in our whitelist.

Taking precautions and not trusting everything online is the best way to protect yourself. Some things you should be cautious about:

- Letting strangers take remote control of your computer. Microsoft will never call you on the phone. Your browser will never tell you to call Microsoft because of malware.
- Opening random email attachments. If you weren't expecting it, be cautious.
- Giving unknown programs and files administrator privileges on your computer. If you didn't open the software or don't trust it, don't give it admin privileges.
- Don't put your credentials in an email. No company will ever ask for your plain text password for any reason. If you get an email claiming your account was locked, always go to a link your trust, don't click the link in the email.

But, how did I get infected in the first place?

It is difficult to track down the source of infection. Most infections are permitted 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 via exploits in your browser or browser plug-ins on websites you visit. Always be very careful what you install. Make sure you trust the source implicitly. When downloading programs, always use the publisher’s website directly.

Revision #4

Created Fri, Nov 13, 2020 4:06 PM by Willzy12h

Updated Mon, Jun 28, 2021 7:51 PM by Ajax146