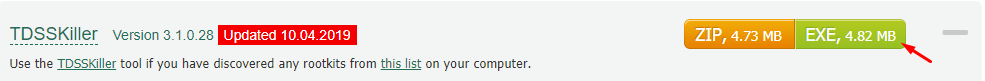
Jonathan Daw

**How to Remove a Rootkit**

**Using Kaspersky TDSSKiller**

Rootkits are a type of malware that give an attacker the ability to install sets of tools to enable constant remote access to your computer. Rootkits can be tricky to locate and identify, because they are usually designed with the intent of staying hidden from the user. Due to the tricky nature of rootkits, Kasperksy has designed a tool specifically for locating and removing rootkits, which is what we will be using today.

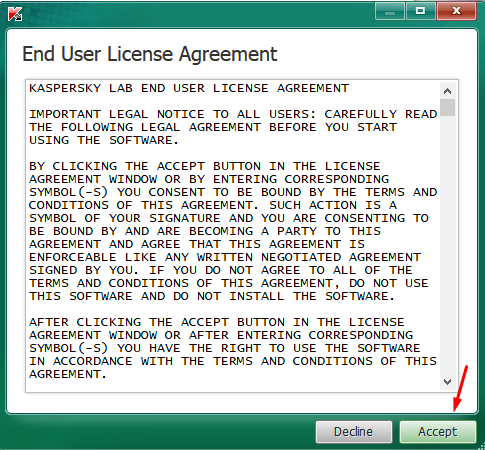
1. Navigate to Kaspersky’s TDSSKiller download page: <https://support.kaspersky.com/viruses/utility#TDSSKiller>
2. Select the .exe file next to the TDSSKiller download



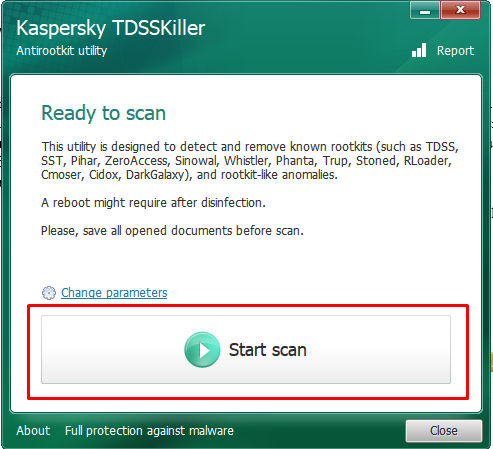
1. Save the TDSSKiller Application wherever you would like



1. Run the application and accept both agreements that pop up



1. Select “Start Scan”



1. Once the scan is complete, the report page will display how many files were scanned and if any were detected as rootkits, they will be removed from the system.

A screenshot of a cell phone

Description automatically generated

**How to Detect and Remove Adware**

**Using Kaspersky Cloud and Resetting Browser Settings**

If you have ever noticed that a significant number of advertisements are displaying on your computer, or your browser keeps redirecting to random products, then you have probably been infected with adware. Adware is a type of malware that causes unwanted advertisements to display on your computer. Adware can we used to steal your information and impacted computer performance. Because adware affects both your computer and your browser, we will be addressing how to handle the quarantining of not only the computer files, but also the settings in your browser.

1. Navigate to Kaspersky’s Security Cloud download page: <https://www.kaspersky.com/downloads/thank-you/free-antivirus-download>
2. Select the “Download Now” button to install the application

A screenshot of a social media post

Description automatically generated

1. Save the application to your desired location
2. Run Kaspersky’s Security Cloud application
3. Make an account with your email to use this product

A screenshot of a cell phone

Description automatically generated

1. You will now see the homepage for the Kaspersky Security Cloud software. In order to remove the adware, we will first need to run a full scan to search the entire computer and remove and potential threats to the device. Select the “Scan” button

A screenshot of a cell phone

Description automatically generated

1. To ensure that the software has the best chance of tracking down the threats and removing them, it is best to update the security databases. Select “Run”

A screenshot of a cell phone

Description automatically generated

1. Once the databases are up to date, it is time to run the Full Scan. Select the “Run scan” button.

A screenshot of a cell phone

Description automatically generated

1. Once the scan is complete, any detected threats will be quarantined and then removed from the system.
2. Now that the computer files have been searched through, it is best to reset the browser settings to ensure that there is no malware left in the system.
3. Open your browser (this guide will be using Google Chrome) and select the customization button in the top right of the browser.

A screen shot of a clock

Description automatically generated

1. Select the “Settings” option to access the various settings in Google Chrome

A screen shot of a monitor

Description automatically generated

1. Because restoring your settings to the default state is not a typical, daily use setting, Chrome has placed the option in the “Advanced” section to ensure a user does not click it unless entirely needed. Scroll down and navigate to the “Advanced” section.

A screenshot of a cell phone

Description automatically generated

1. Scroll all the way to the bottom of the page under the “Reset and clean up” section to find what we are looking for. Select “Restore settings to their original defaults.”

A picture containing sitting

Description automatically generated

1. Finally, confirm the restoration by selecting “Reset Settings”

A screenshot of a cell phone

Description automatically generated

**How to Use System Restore to Remove a Virus**

**For Windows 10**

A Windows System Restore is a strong, simple answer to removing a virus on your system. Before any important updates or other events, your computer will save a restore point, so that if any issues occur, you can safely restore back to that point in time and continue with normal operations. This is useful for ridding of an unwanted virus on your device because it allows us to travel back to before our device was infected. Follow these steps to restore your system to a point before infection:

1. Right-click on the Windows start button in the bottom left of your screen and select the search option.

A screenshot of a cell phone

Description automatically generated

1. Type “Recovery” into the search bar to find the Recovery section of the Control Panel. This is where we will navigate to the System Restore section.

A screenshot of a cell phone

Description automatically generated

1. Select Open System Restore page to begin the process

A screenshot of a cell phone

Description automatically generated

1. We are going to look at the available restoration points to see which point will work for our system. Select the “Choose a different restore point” radio button.A screenshot of a social media post

   Description automatically generated

<https://www.youtube.com/watch?v=8tgodWHzApo>

1. Select “Show more restore points” to view all of the possible restoration points. Start by selecting the most recent restoration point. Once we restore the system, if the issue is not resolved, repeat each step, and choose the next restoration point on the list. Repeat this process until the issue is resolved and the virus is no longer on the system.

A screenshot of a cell phone

Description automatically generated

<https://www.youtube.com/watch?v=8tgodWHzApo>

1. Select the desired restoration point and go to the next page to finish the System Restore

A screenshot of a cell phone

Description automatically generated

<https://www.youtube.com/watch?v=8tgodWHzApo>

1. To finish the process and restore our system to a previous point, select the “Finish” button and confirm the action by selecting “Yes.”

A screenshot of a cell phone

Description automatically generated

<https://www.youtube.com/watch?v=8tgodWHzApo>

1. Now that your system is restored to a previous point, ensure that the virus has been removed. If this restoration point was not far back enough, repeat the process and select a restoration point that is further back in time.