

Remove Poweliks Virus

1. Close all applications and save your work. Running these steps in the order below is necessary.
2. Download and run Process Explorer as an administrator
3. Download and run the latest version of RogueKiller
4. Let RogueKiller initialize and then click the Scan button. RogueKiller will automatically open the help page on how to remove Poweliks if it finds an infection or a thank you page for using RogueKiller if you're using it for the first time. Close those windows if they pop up. Once the scan is complete, navigate to the Registry tab in RogueKiller and scroll to the bottom. You should see the a line item in red like the screenshot below if your system has been infected:

NOTE: RogueKiller is known to incorrectly identify malicious programs and hijacks on computers from time to time, so I recommend only checking the box next to the Poweliks infection before clicking Delete.
5. Get ready to hit DELETE in RogueKiller, BUT DON'T CLICK IT JUST YET.
6. Using Process Explorer, scroll through your active process list and locate a varying number of dllhost processes. Right-click the root process and select Kill Process Tree. YOU'LL SEE A PROMPT ASKING IF YOU ARE SURE YOU WANT TO KILL THE SELECTED PROCESS TREE, click YES.
7. Now click DELETE in RogueKiller and reboot the system immediately. It is important to reboot the system before the Trojan re-launches and puts itself back into the registry. **NOTE:** This Trojan also runs in Safe-Mode with networking.
8. In some cases the Trojan can be responsible for creating a large amount of data in C:\users\\appdata\local\temp\. I recommend removing this data with CCleaner available here: <https://www.piriform.com/ccleaner/builds>