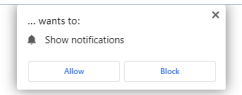
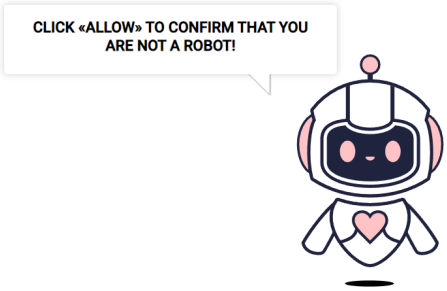
Top-Captcha:Malware Description

These threats take place on bait websites that mimic real sites using methods such as typosquatting and spoofing. The goal of these threats are for you to allow them to send you notifications on google which will also be sent directly to your device. Once the threat gets the ability to send notifications it will spam your device saying you have a virus mimicking microsoft defender or google in most instances. The end goal of the attack is for you to run the “Virus Scan” and allow them to install malicious malware onto your system, which I found in some instances to take advantage of your graphics card attempting to mine crypto currency.

Threat Defense

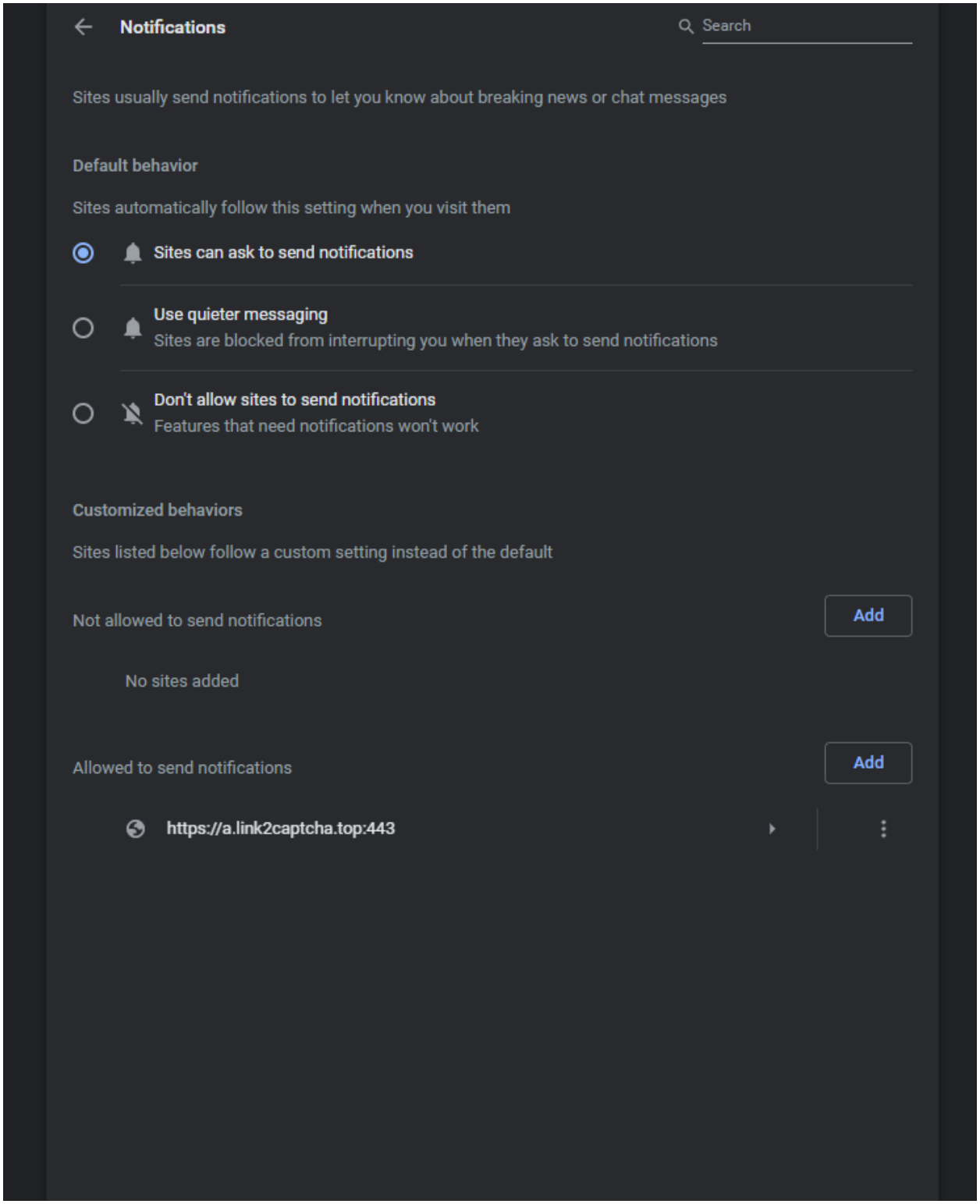
Ex: Botcon Video



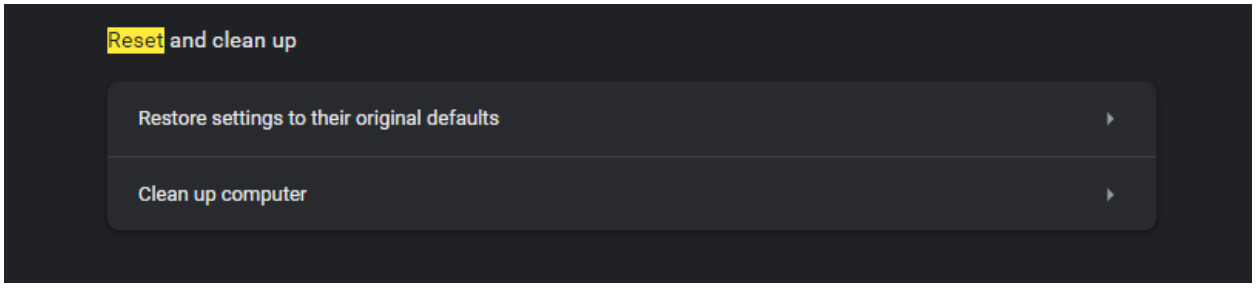


Refer to the resources below and install each of them respectively. First check your allowed notifications in google by doing the following: Settings(top right) > Privacy and Security > Site

Settings > Notifications > check sites in the “Allowed to send notifications” tab then remove the site named a.link2captcha.top.



The rest of the steps are only necessary if you have restarted your system since you allowed the notifications. Now you can open Malwarebytes and run a basic scan, which can take anywhere from 1-5 minutes depending on the amount of info on your system. Once your Malwarebytes scan has finished you can begin a scan with HitmanPro, which can take 1-5 minutes also depending on the amount of info on your system. Once that scan has finished you can go to settings and search reset to help clean up your browser and system.



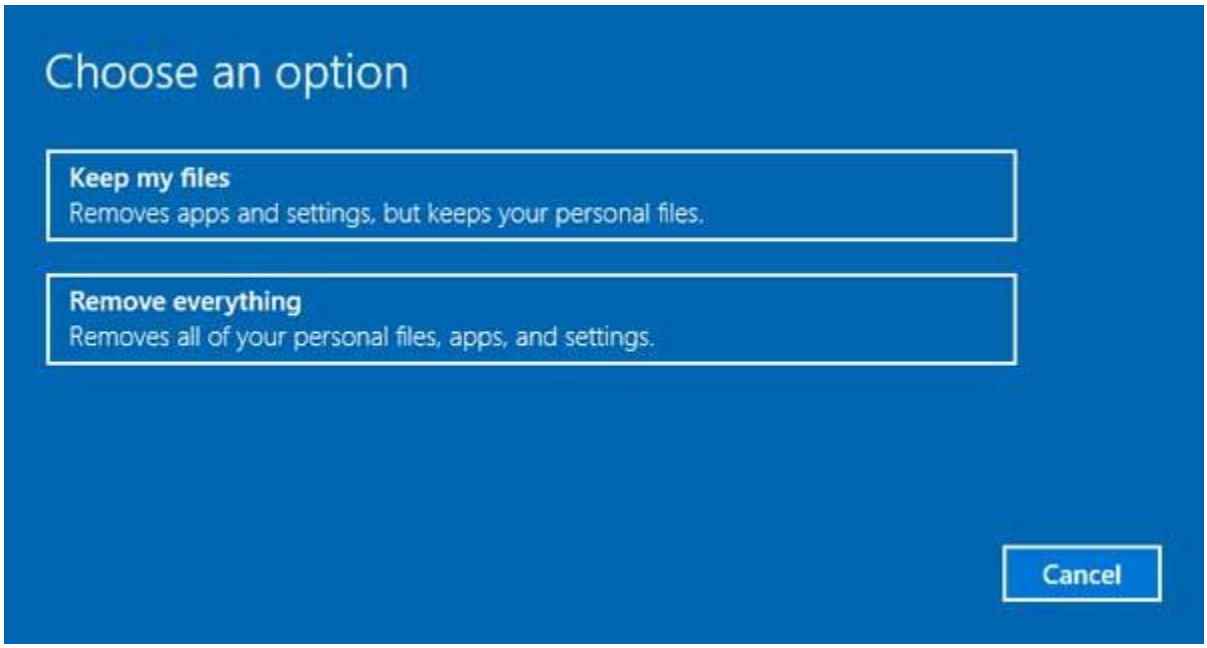
If you caught the threat early by this point the malware should be completely erased from your system.

In the event that you clicked run on this notification.

You should refer back to Malwarebytes and try to identify the threat, which is a trojan virus, more specifically a form of crypto mining malware that will utilize a majority of your graphics card to mine crypto currency discreetly. The easiest way to identify crypto mining being present is running a benchmark test focused on your model of graphics card, a link will be in the

description with a suggestion. This test will test the FPS your card is generating and by searching on google you can compare your average FPS to the FPS that is standard with the test.

The first solution to getting rid of this malware is to reset your system either entirely or keeping personal files as shown below.



Keeping your files will keep any text documents you may have created along with installers and is generally less complicated, but in this situation less effective due to the virus potentially still remaining. Removing everything will do what it says and guarantee the eradication of the virus along with anything else on the system. After resetting your system you have now entirely erased the virus' good job, now you just need to reinstall everything onto your system.

Resources and more

Malwarebytes:https://www.malwarebytes.com/mwb-download

HitmanPro:https://www.hitmanpro.com/en-us

Pc Reset

Guide:https://support.microsoft.com/en-us/windows/give-your-pc-a-fresh-start-0ef73740-b927-549b-b7c9-e6f2b48d275e#:~:text=To%20reset%20your%20PC%2C%20go%20to%20Start%20%3E%20Settings%20%3E%20Update,Reset%20this%20PC%20%3E%20Get%20Started.

Benchmark:https://gpu.userbenchmark.com/Software