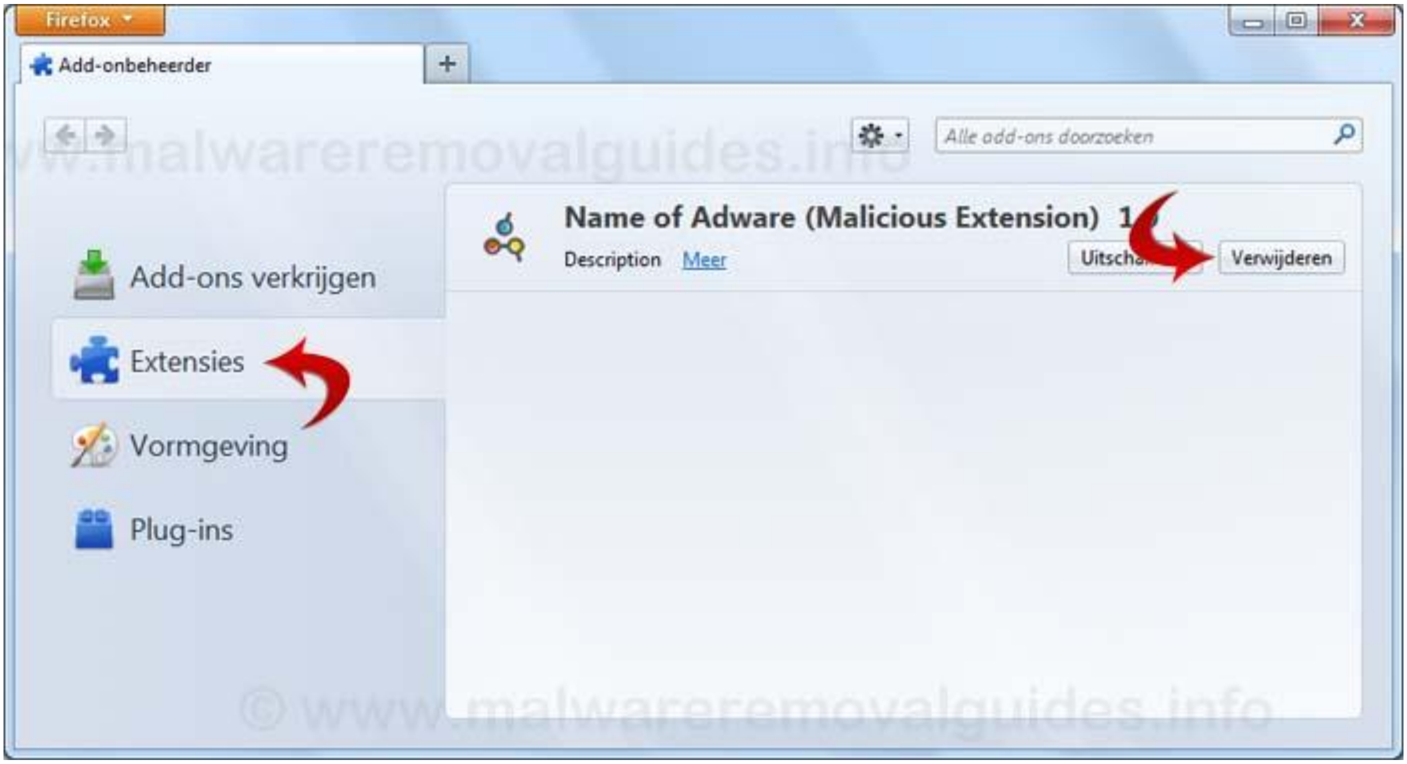
How to remove Adware from Mozilla Firefox

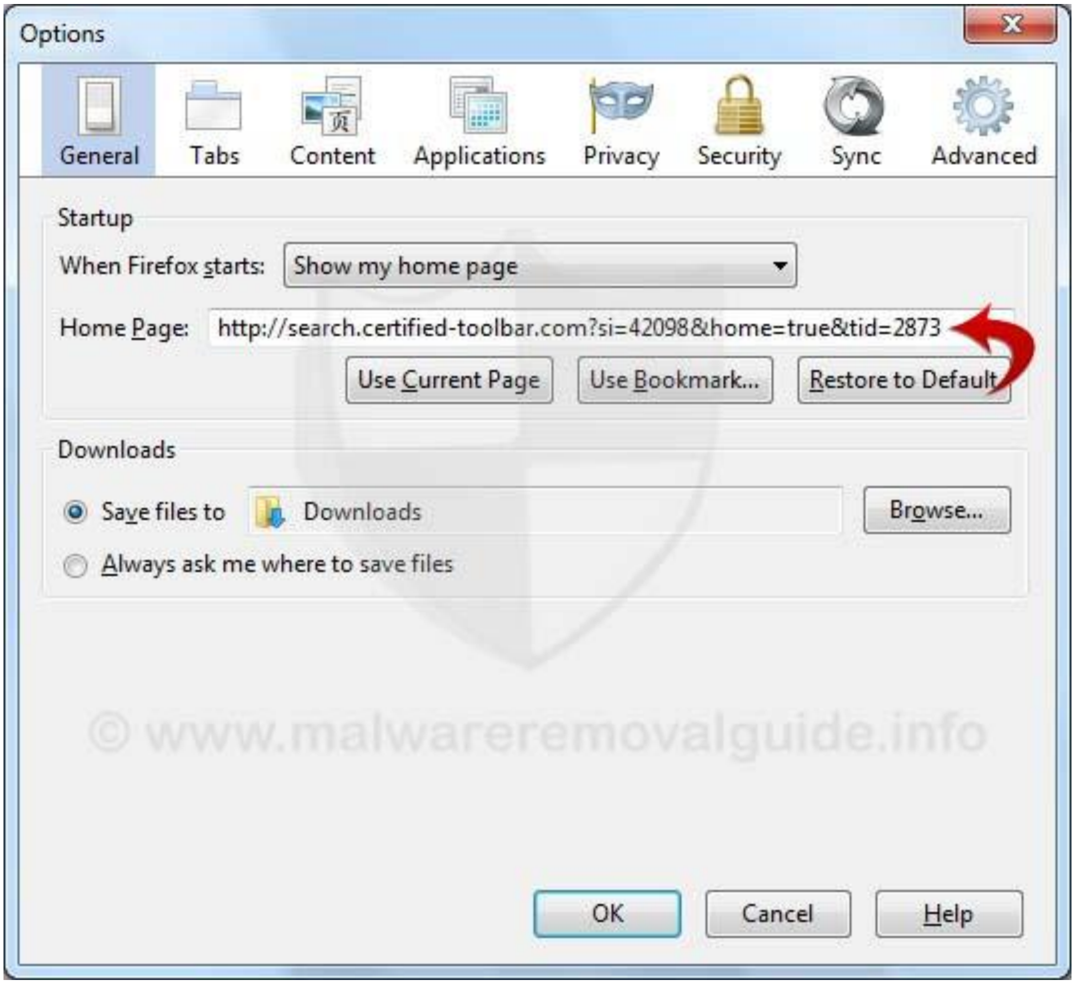
Mozilla Firefox is one of the most popular browsers, and therefore also a popular target for installing adware and other untwanted extensions. In this article "How to remove Adware from Mozilla Firefox" we will explain how to easily remove any adware or *Potentially Unwanted Programs* from Mozilla Firefox.
When Mozilla Firefox is affected by unknown extension or adware, you may experience frequent pop-up ads and redirects to malicious domains. Remove any adware or *Potentially Unwanted Programs* from Mozilla Firefox using the guide below. We recommend strongly to create a systemrestore point before you start with re removal proces.

How to remove Adware from Mozilla Firefox

- Start Firefox and Press **Ctrl+Shift+A** on your keyboard to open the **'Add-Ons Manager'**. This windows will provide a list of all extensions and plugins installed in Firefox.
- Under **Extensions**, select the adware or *Potentially Unwanted Program* items and the click the **Remove** button.
- If Firefox prompts to **'Restart Now'**. Please restart Firefox and check if the changes you have made are successful.



- Press the Firefox button and then select **options** and reset the default homepage on the **General Tab**



When Firefox starts: Show my home page

Home Page: http://search.certified-toolbar.com?si=42098&home=true&tid=2873

● Save files to Downloads

○ Always ask me where to save files

- At the top of the Firefox window, click the **Firefox button**, go over to the **Help** sub-menu (on *Windows XP*, click the Help menu at the top of the Firefox window), and select **Troubleshooting Information**.
- Click the **Reset Firefox** button in the upper-right corner of the *Troubleshooting Information* page.
- Click **Reset Firefox** in the confirmation window that opens.
- Firefox will close and wil be reset with the default settings.
- When it’s done, a window will list the information that was imported. Click **Finish** and check everything is fixed as well.

How to remove Adware from Mozilla Firefox

All tools used in our malware removal guides are completely free to use and should remove any trace of malware from your computer.

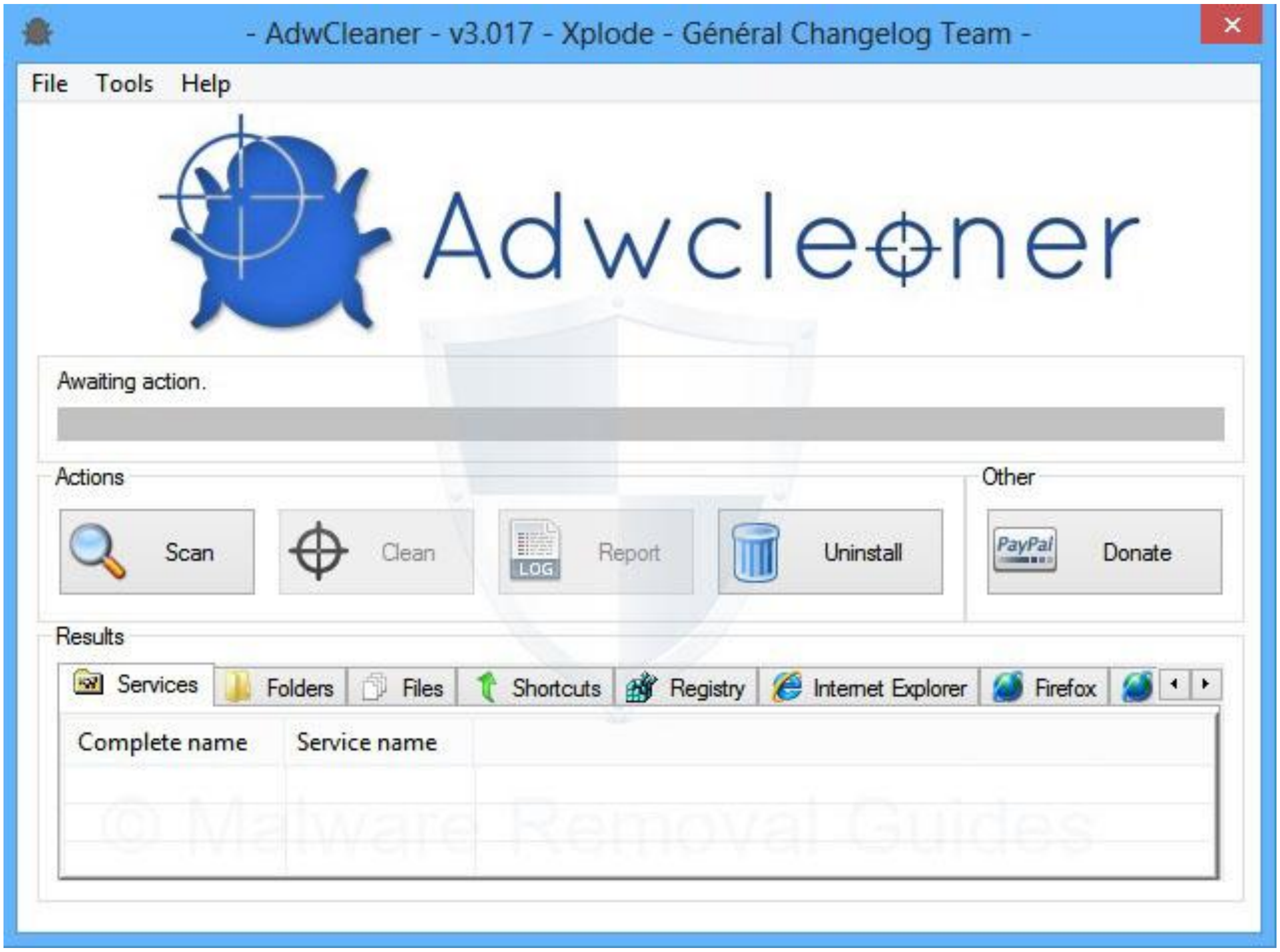
Please be aware that removing Malware is not so simple, and we strongly recommend to backup your personal files and folders before you start the malware removal process.

Malwarebytes
DETECTS & DESTROYS ZERO-HOUR MALWARE YOUR ANTIVIRUS MISSES.
DOWNLOAD
CNET Editors' Rating
Outstanding
Community Powered & Expert Trusted

1. Run a scan with AdwCleaner to remove the Adware

Download

- Download **AdwCleaner** (*from the download button above*) to your desktop.
- **Important!** Before starting AdwCleaner, close all open programs and internet browsers.
- Double click on **AdwCleaner.exe** to start the program
- **Windows Vista**/ **7/8** users right-click and select **Run As Administrator**.
- Click on the scan **button**,
- When the scan is ready click on the **Clean** butten.



Awaiting action.

- Your desktop icons will be disappear, this is normal so don’t be worry about that.
- Press **OK** when asked to close all programs and follow the onscreen prompts.
- Press **OK** again to allow AdwCleaner to restart the computer and complete the removal process.
- Close the text file that opens after the restart, double click on **adwcleaner.exe** to run the tool.
- Click now on **Uninstall**, then confirm with **yes** to remove AdwCleaner from your computer.

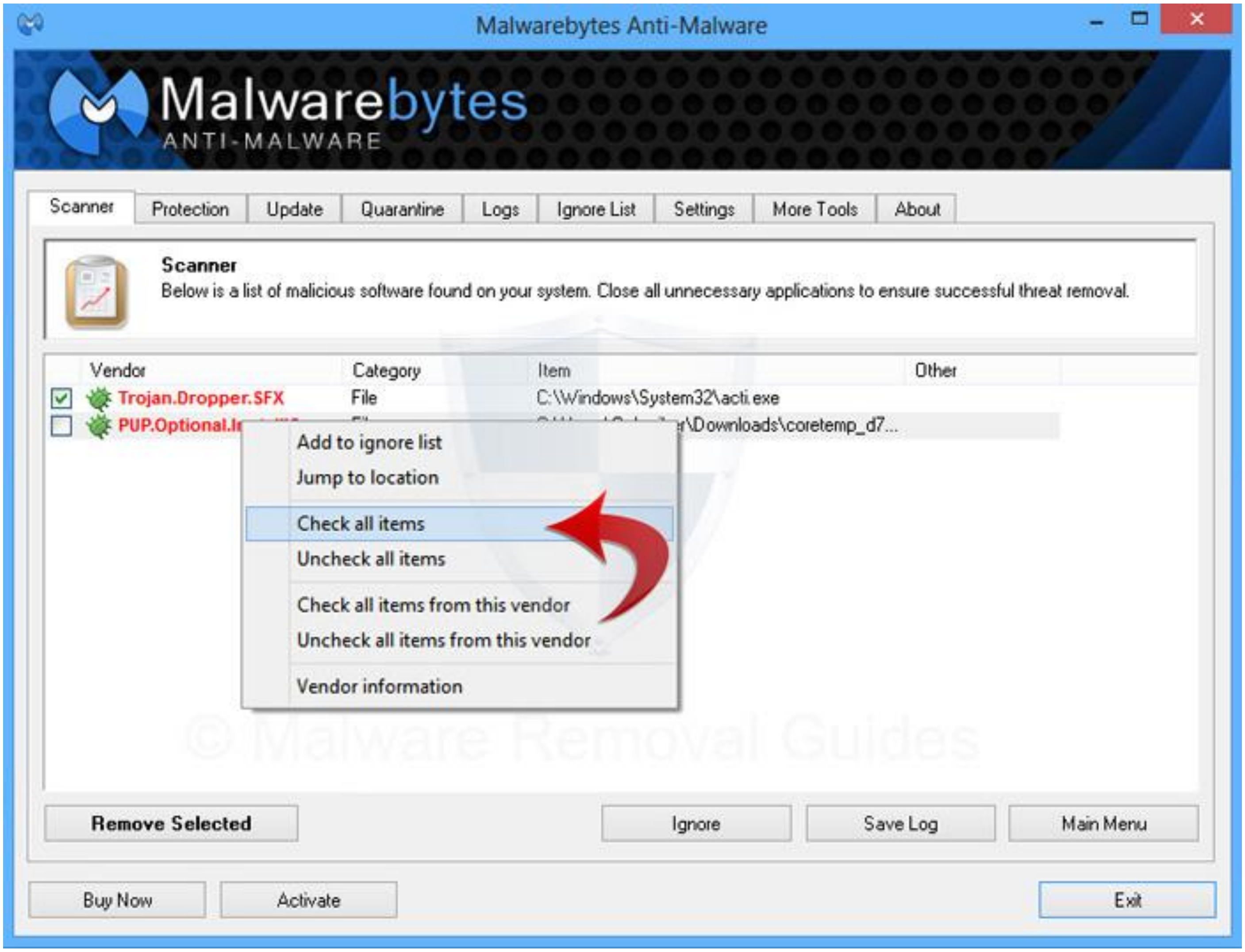
2. Run a scan with Malwarebytes Anti-Malware

Malwarebytes Anti-Malware (*MBAM*) is a surprisingly effective **anti-malware** program that let you check the presence of malware. But Malwarebytes has also a very strong detection of Potentially Unwanted Programs (*PUP’s*), only the PUP detection will show up unchecked on the results list by default. You have to manually check them for removal.

Tip: If you want more advanced features and the real-time protection you can purchase the full version of Malwarebytes Anti-Malware that will protect you from being infected.

- Download **Malwarebytes Anti-Malware** (*from the download button above*) to your desktop.

- Double-click **mbam-setup.exe** and follow the prompts to install the program.
- At the end, be sure a checkmark is placed next to **Update Malwarebytes' Anti-Malware** and **Launch Malwarebytes' Anti-Malware**
- Then click **Finish**. If an update is found, it will download and install the latest version.
- Once the program has loaded, select **Perform full scan**, then click **Scan**.
- When the scan is complete, click **OK**, then **Show Results** to view the results.
- Be sure that everything is Checked (ticked) and click on **Remove Selected**.
- You can use the right mousbutton to check the '**Check all items**' option before you click on Remove Selected



Scanner

Below is a list of malicious software found on your system. Close all unnecessary applications to ensure successful threat removal.

	Vendor	Category	Item	Other
☑	Trojan.Dropper.SFX	File	C:\Windows\System32\acti.exe	
□	PUP.Optional.In		\Downloads\coretemp_d7...	

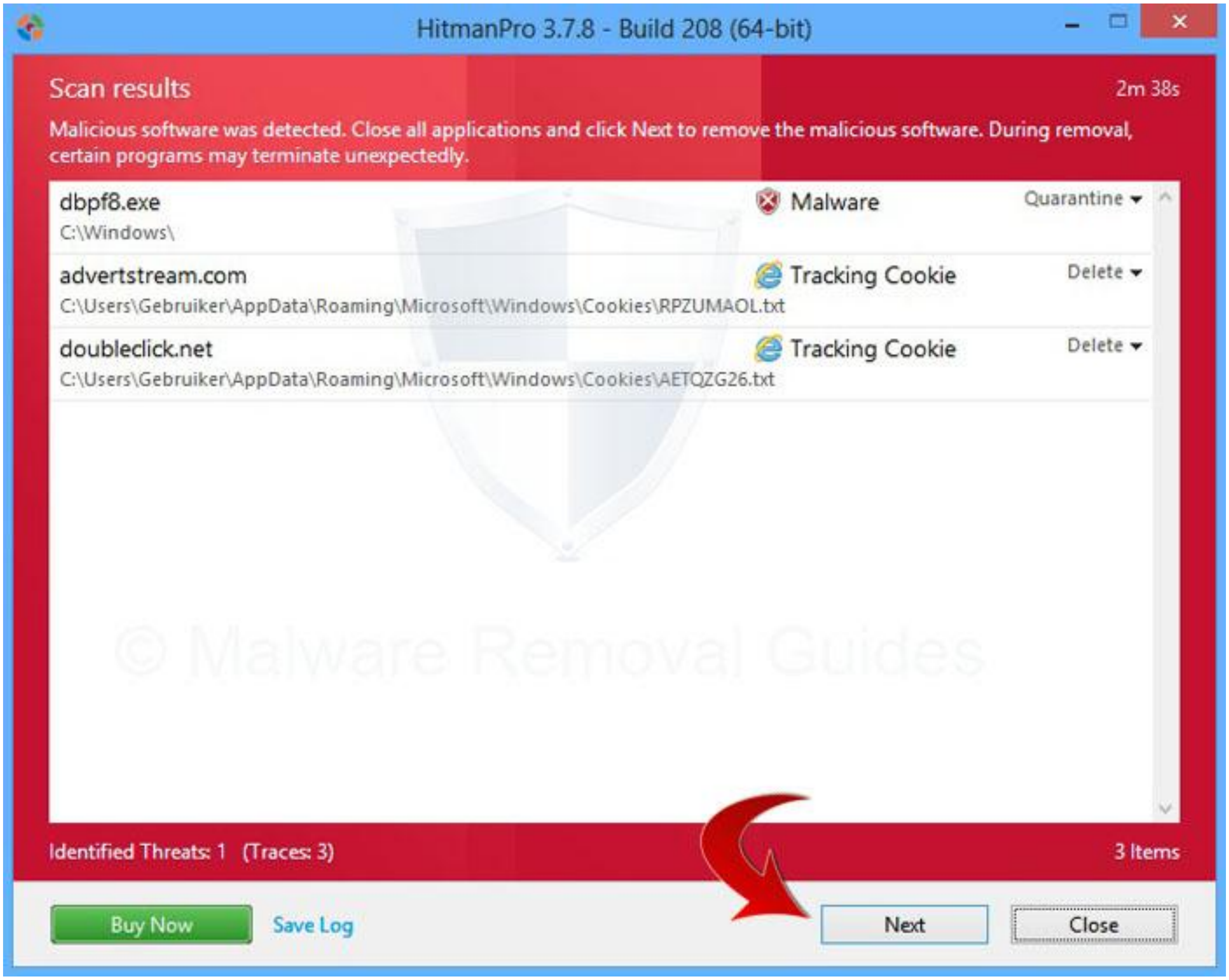
- When removal is completed, a log report will open in Notepad.
- If you accidently close it, the log is automatically saved and can be viewed by clicking the Logs tab.
- ***Note**: If MBAM encounters a file that is difficult to remove, you will be presented with 1 of 2 prompts.*
- Click OK to either and let MBAM proceed with the disinfection process.

- If asked to restart the computer, please do so immediately. Failure to reboot will prevent MBAM from removing all the malware.
- After the restart in **Normal mode**, start **Malwarebytes Anti-Malware** again and **perform a Quick scan** to verify that there are no remaining threats.

3. Run a scan with HitmanPro to remove remnants of adware

Download - 32 bit Download - 64 bit

- Please download **HitmanPro** to your desktop from one of the download buttons above.
- Double click on HitmanPro to start the program, if you are experiencing problems while trying to start HitmanPro, you can use the ***Force Breach*** mode.
- To start HitmanPro in Force Breach mode, **hold down the left CTRL-key when you double click on HitmanPro**and all non-essential processes will be terminated, including the malware processes.
- HitmanPro will start and you'll need to follow the prompts (by clicking on the **Next** button) to start a system scan with this program.
- The program will start to scan the computer. The scan will typically take no more than 2-3 minutes.
- Click on the next button and choose the option **activate free license**
- Click on the next button and the infections where will be deleted.
- Click on the next button and restart the computer.



HitmanPro 3.7.8 - Build 208 (64-bit)

Scan results

2m 38s

Malicious software was detected. Close all applications and click Next to remove the malicious software. During removal, certain programs may terminate unexpectedly.

dbpf8.exe C:\Windows\	Malware	Quarantine
advertstream.com C:\Users\Gebruiker\AppData\Roaming\Microsoft\Windows\Cookies\RPZUMAOL.txt	Tracking Cookie	Delete
doubleclick.net C:\Users\Gebruiker\AppData\Roaming\Microsoft\Windows\Cookies\AETQZG26.txt	Tracking Cookie	Delete

Identified Threats: 1 (Traces: 3)

3 Items

: