## **Remove ANY TOOLBAR from Internet Explorer, Firefox and Chrome**

Browser toolbars have been around for years, however, in the last couple of months they became a huge mess. Unfortunately, lots of free software comes with more or less unwanted add-ons or browser toolbars.

These are quite annoying because they may:

- Change your homepage and your search engine without your permission or awareness
- Track your browsing activities and searches
- Display annoying ads and manipulate search results
- Take up a lot of (vertical) space inside the browser
- Slow down your browser and degrade your browsing experience
- Fight against each other and make normal add-on handling difficult or impossible
- Become difficult or even impossible for the average user to fully uninstall

Toolbars are not technically not a virus, but they do exhibit plenty of malicious traits, such as rootkit capabilities to hook deep into the operating system, browser hijacking, and in general just interfering with the user experience. The industry generally refers to it as a "PUP," or potentially unwanted program.

Generally speaking, toolbars are ad-supported (users may see additional banner, search, pop-up, pop-under, interstitial and in-text link advertisements) cross web browser plugin for Internet Explorer, Firefox and Chrome, and distributed through various monetization platforms during installation. Very often users have no idea where did it come from, so it's not surprising at all that most of them assume that the installed toolbar is a virus.

For example, when you install iLivid Media Player, you will also agree to change your browser homepage to *search.conduit.com*, set your default search engine to *Conduit Search*, and install the AVG *Search-Results Toolbar*.

However when you uninstall iLivid Media Player from your computer, your web browser's default settings will not be restored. This means that you'll have to remove *search.conduit.com* and from your favorite web browser manually.

The most common toolbar infections that can be found on the Internet are:

- Ask.com Toolbar
- Yahoo! Toolbar
- Mail.ru toolbar

- Babylon Toolbar
- SweetPacks Toolbar
- Delta Toolbar
- Searchqu Toolbar
- Sweet IM Toolbar
- DealPly Toolbar
- Funmoods Toolbar
- Softonic Toolbar
- Yontoo Toolbar
- Snap.Do Toolbar
- IMinent Toolbar
- PriceGong Toolbar

You should **always pay attention when installing software** because often, a software installer includes optional installs, such as these toolbar. Be very careful what you agree to install.



**Always opt for the custom installation** and deselect anything that is not familiar, especially optional software that you never wanted to download and install in the first place. It goes without saying that you should not install software that you don't trust.

### How to remove ANY Toolbar from Internet Explorer, Firefox and Chrome (Virus Removal Guide)

This page is a comprehensive guide, which will remove ANY Toolbar from Internet Explorer, Firefox and Google Chrome.

Please perform all the steps in the correct order. If you have any questions or doubt at any point, **STOP** and ask for our assistance.

**STEP 1**: Uninstall ANY Toolbar malicious programs from your computer

STEP 2: Remove ANY Toolbar from Internet Explorer, Firefox and Chrome

**STEP 3**: Remove ANY Toolbar adware with AdwCleaner

STEP 4: Remove ANY Toolbar browser hijackers with Junkware Removal Tool

STEP 5: Remove Toolbar virus with Malwarebytes Anti-Malware Free

**STEP 6**: Double-check for the Toolbar infection with HitmanPro

## **STEP 1 : Uninstall Toolbar program from your computer**

Most toolbars will install a program on your computer, while this is not a general rule, we will need to check for any malicious programs. In this first step, we will try to identify and remove any malicious program that might be installed on your computer.

1. To uninstall the **toolbar** program from your computer, click the Start button, then select **Control Panel**, and click on **Uninstall a program.** 

If you are using Windows 8, simply drag your mouse pointer to the right edge of the screen, select Search from the list and search for "*control panel*". Or you can right-click on a bottom left hot corner (formerly known as the Start button) and select **Control Panel** from there, then select *Uninstall a program*.



2. When the Add/Remove Programs or the Uninstall a Program screen is displayed, scroll through the list of currently installed programs and uninstall any recently installed or unknown programs from your computer.

The most common programs installed on users computers are: BitGuard, Delta Toolbar, DefaultTab, Search Protect by Conduit, Ask toolbar, Babylon Toolbar, Browser Protect, WebCake, Mixi.DJ toolbar and many others. As a general rule, if you have not installed a

nro	arom	and	dan'i	t lon and	what it	daaa	you chould	uningtall	it from	1/011#	0000	autor
DIO	21am	anu	uon	LKHOW	what h	uoes.	vou snouia	unnistan	ппош	vou	COIIII	Julei.
							J = ++ === = ++ = ++					

Programs and Features	All Control Panel Items      Program	ns and Features		*	49
Control Panel Home View installed updates View Turn Windows features on or off	Uninstall or change a p To uninstall a program, select Organize 👻 Uninstall	rogram it from the list and the	n click Uninstall, C	ihange,	or f
	Name	Publisher	Installed On	Size	
	@FLV Player	Somoto Ltd.	8/19/2013		243
	AppsHat Mobile Apps	Somoto Ltd.	8/19/2013		
	Web-Cake 3.00	Web Cake LLC	8/19/2013	1	
	LyricsSay-1	LyricsSay-1	8/19/2013		
	Bundled software uninstaller		8/19/2013		
	Optimizer Pro v3.0	PC Utilities Pro	8/19/2013	2	28.0
	🐞 FilesFrog Update Checker	are inpa	8/19/2013		
	Babylon Chrome Toolbar	Babylon Ltd.	8/19/2013		

If you are having issues while trying to uninstall the Toolbar, you can use **<u>Revo Uninstaller</u>** to completely remove this unwanted program from your machine.

Depending on what program has installed the unwanted Toolbar, the above program may have a different name or not be installed on your computer.

If you cannot find any unwanted or unknown programs on your machine, then you can proceed with the next step.

### **STEP 2 : Remove Any Toolbar from Internet Explorer, Firefox and Chrome**

#### **Remove Any toolbar from Internet Explorer**

You can reset Internet Explorer settings to return them to the state they were in when Internet Explorer was first installed on your PC.

1. Open Internet Explorer, click on the "gear icon" 🔯 in the upper right part of your browser, then click again on Internet Options.



2. In the "*Internet Options*" dialog box, click on the "**Advanced**" tab, then click on the "**Reset**" button.

	General Security Privacy Content Connections Programs Advanced
	Settings nectați-vă
Gc	Accelerated graphics Use software rendering instead of GPU rendering* Always expand ALT text for images Enable Caret Browsing for new windows and tabs Move system caret with focus/selection changes Play system sounds Reset text size to medium for new windows and tabs Reset zoom level for new windows and tabs Browsing Close unused folders in History and Pavorites* Disable script debugging (Internet Explorer) Disable script debugging (Other) Disable script debugging (Other) Traise effect after you context you commuter
Cáutare Goci Google.ro oferit i	Reset Internet Explorer settings Resets Internet Explorer's settings to their default condition. You should only use this if your browser is in an unusable state.

3. In the "*Reset Internet Explorer settings*" section, select the "**Delete personal settings**" check box, then click on "**Reset**" button.



4. When Internet Explorer has completed its task, click on the "**Close**" button in the confirmation dialogue box. You will now need to close your browser, and then you can

open Internet Explorer again.



#### **Remove Any Toolbar from Mozilla Firefox**

If you're having problems with Firefox, resetting it can help. The reset feature fixes many issues by restoring Firefox to its factory default state while saving your essential information like bookmarks, passwords, web form auto-fill information, browsing history and open tabs.

1. In the upper-right corner of the Firefox window, click the **Firefox menu button** (**=**), then click on the "**Help**" (**?**) button.

Google +		
A https://www.google.rg	V C Soogle	₽☆₿₩₩≣
	+Drs. Google România Câutare Google Mă simt norocos	X     Cut     Image: Copy     Paste       -     100%     +       Image: Copy     Image: Copy     Image: Copy       Image: Copy     Image: Copy     Image: Copy
		🖬 Customize 🔍 🖒
Publicitate Companii Despre	Confidențialitate și termeni a	rctualizați Setări Folosiți Google.com

2. From the *Help* menu, choose **Troubleshooting Information**. If you're unable to access the Help menu, type *about:support* in your address bar to bring



up the Troubleshooting information page.

3. Click the "**Reset Firefox**" button in the upper-right corner of the "*Troubleshooting Information*" page.

about:support					C 3	<ul> <li>Google</li> </ul>	p	☆	e	+	Ĥ	
Troublesh	ooting	Informa	tion		4						-	
This page contains te you are looking for a	chnical inform nswers to com	ation that might I mon questions ab	be useful when you'n out Firefox, check ou	trying to solve a problem t our <u>support website</u> .	¥	Reset Firefox	to its defau mejor problem h with only yo	u <b>lt sta</b> is whic iur esse	i <b>te</b> :h you ential	canit		
Copy raw data to	clipboard	Copy text to cl	ipboard			information.		_				
							Reset Firefo	5				
Application B	lasics											
Name	Firefox											
Version	29.0											
Update History	Show Up	date History										
User Agent	Mozilla/5.0 (V	Windows NT 6.1; \	WOW64; nr.29.0) Geck	a/20100101 Firefax/29.0								
Profile Folder	Show Fol	der										
	aboutplugin											
Enabled Plugins												
Enabled Plugins Build Configuration	aboutbuilde	onfig										

4. To continue, click on the "**Reset Firefox**" button in the new confirmation window that opens.

about:support				G	Goog - Goog	ie	p	ម	E	*	π
Troublesh This page contains te you are looking for an	ooting I chnical informati iswers to commo	on that might	ation be useful when you're trying to solve a problem. B bout Firefox, check out our <u>support website</u> .	Y	Rese	t Firefox	to its defa	ult sta	n <b>te</b> th you o	can't	Î
Copy raw data to clipboard Copy text to		Copy lest to	Neset Firefox	set Firefox ve, start tresh with only your mation.				Jui ess	cnual		
Application B	Application Basics		Firefox will try to preserve your: Windows and Tabs Browsing History and Bookmarks Saved Passwords				Resetrited	JX.			
Name	Firefox		Saved Form History								
Version	29.0		Cookes Firefox will restart and everything else will b	erem	oved.				_		
Update History	Show Upda	te History									
User Agent	Mozilla/5.0 (Wi	ndows NT 6.1	Neset Therox	Can	CEL						
Profile Folder	Show Folde	я									
Enabled Plugins	about plugins										
<b>Build</b> Configuration	aboutbuildcon	fig									
Memory Use	aboutmemory										
Crach Penort	for the La	et 3 Dave									

5. Firefox will close itself and will revert to its default settings. When it's done, a window will list the information that was imported. Click on the "**Finish**".

**Note**: Your old Firefox profile will be placed on your desktop in a folder named "*Old Firefox Data*". If the reset didn't fix your problem you can restore some of the information not saved by copying files to the new profile that was created. If you don't need this folder any longer, you should delete it as it contains sensitive information.

#### **Remove Any Toolbar from Google Chrome**

1. Click on Chrome's main menu button, represented by three horizontal lines ( ). When the drop-down menu appears, select the option labeled **Settings**.

					\$
	New tab				Ctrl+T
	New window				Ctrl+N
	New incognito window			Ctrl+	Shift+N
eı	Bookmarks				
	Recent Tabs				
	Edit		Cut	Сору	Paste
	Zoom	2	1009	6 +	23
	Save page as				Ctrl+S
	Find				Ctrl+F
	Print				Ctrl+P
iä	Tools				
_	History				Ctri+H
	Downloads				Ctrl+J
1	Signed in as malwaretips@	gmail.c	om	8	
	Settings				
	About Google Chrome				
+124	Help				
	Exit			Ctrl+	Shift+Q
and the second se					

2. Chrome's Settings should now be displayed in a new tab or window, depending on your configuration. Next, scroll to the bottom of the page and click on the **Show advanced** 

settings link (as seen in the below example).

			-
Settings	* Chrome//settings		54
	Concret/seconds		24
Chrome	Settings	Search settings	
listory	Sign in		
xtensions	Signed in as malwaretips@gmail.com. Manage your synced data on Google Dashboard.		
lettings	Disconnect your Google Account Advanced sync settings		
teln	On startup		
roop.	Open the New Tab page		
	Continue where I left off		
	Open a specific page or set of pages. Set pages		
	Appearance		
	Get themes Reset to default theme		
	Chan Hame butten		
	New Tab page Change		
	Always show the bookmarks bar		
	Search		
	Set which search engine is used when searching from the omnibox.		
	Google   Manage search engines		
	Users		
	You are currently the only Google Chrome user.		
	Add new user Delete this user Import bookmarks and settings		
	Default browser		
	The default browser is currently Google Chrome.		
	Show advanced selftings		
	<b>W</b>		

3. Chrome's advanced Settings should now be displayed. Scroll down until the *Reset browser settings* section is visible, as shown in the example below. Next, click on the

#### **Reset browser** settings button.

Chrome	Settings	Search settings
History	Ask where to save each file before downloading	
Extensions		
Settings	HTTPS/SSL	
	Manage certificates	
Help	Check for server certificate revocation	
	Google Cloud Print	
	Set up or manage printers in Google Cloud Print. Learn more	
	Manage	
	Show notifications when new printers are detected on the network	
	System	
	Continue running background apps when Google Chrome is closed	
	Use hardware acceleration when available	
	Reset browser settings	
	Restore browser settings to their original defaults.	
	Reset browser settings	

4. A confirmation dialog should now be displayed, detailing the components that will be restored to their default state should you continue on with the reset process. To complete

- ⇒ C fi	chrome://settings/resetProfileSettings	☆	Ξ
	Settings Sealch satings		
	Ack where to save each file before downloading		
	HTTPS/SSL		
	Google ()   Set us   Set us   Your browser settings will be restored to their original defaults. This will reset your homepage, new tab page and search engine, disable your extensions and unpin all tabs. It will also clear other temporary and cached data, such as cookies, content and site data.   Learn more   System   Image: Complete Chrome better by reporting the current settings Image:		
	Reset browser settings Restore browser settings to their original defaults. Reset browser settings		

the restoration process, click on the **Reset** button.

# **STEP 3: Remove ANY Toolbar adware from your computer with AdwCleaner.**

The AdwCleaner utility will scan your computer and web browser for malicious files, adware browser extensions and registry keys, that may have been installed on your computer without your knowledge.

- 1. You can **download AdwCleaner** utility from the below link. <u>ADWCLEANER DOWNLOAD LINK</u> (*This link will automatically download AdwCleaner on your computer*)
- 2. Before starting AdwCleaner, close all open programs and internet browsers, then double-click on the AdwCleaner icon.



If Windows prompts you as to whether or not you wish to run AdwCleaner, please allow it to run.

3. When the AdwCleaner program will open, click on the "**Scan**" button as shown below.

-0-	Ad	JUU	ea	ner
Awaiting action.				
Actions	Clean	Report	Uninstal	Other PayPal Donate
Results           Image: Services	Folders 🗇 Files 🐧	Shortcuts 💣 Registry	🏉 Internet Explor	er 🍯 Firefox 🍯 🖅
Complete name	Service name			

AdwCleaner will now start to search for any malicious files that may be installed on your computer.

4. To remove the malicious files that were detected in the previous step, please click on the "Clean" button.

Tools Help			
* A	JwC	lea	∩er
ending. Please uncheck elements	you don't want to remove.		
ctions			Other
Q			Ph. Pal
Scan 🌾 🖓	lean Report	Uninstall	Donate
icaulta	1.4	1.00	
Services 5 Folders	Files C Shortcuts	Registry 🦰 Internet Explo	irer 🥔 Firefox 🧔 付 👌
Path			
C:\Program Files (x86)\Free	ven pro 1.2		
C:\Program Files (x86)\New	/Player		
C:\Program Files (x86)\Sear	chProtect		
C:\Program Files (x86)\Tidy	Network		
C:\Program Files (x86)\Unin	ıstaller		
C:\Users\MalwareTips\Appl	Data\Local\SearchProtect		
C:\Users\MalwareTips\Appl	Data\Local\TidyNetwork		
C:\Users\MalwareTips\Appl	Data\Roaming\Mozilla\Fire	fox\Profiles\wbbyeizb.de	fault\Extensions\tidynetw
C:\Users\MalwareTips\Appl	Data\Roaming\Mozilla\Fire	fox\Profiles\wbbyeizb.de	fault\Extensions\2ab9302
C:\Users\MalwareTips\Appl	Data\Roaming\Mozilla\Fire	fox\Profiles\wbbyeizb.de	fault\Extensions\a0046b9t
C:\Users\MalwareTips\Appl	Data\Local\Google\Chrom	e\User Data\Default\Exte	nsions\dmgpbjjcdccinnnc
4	40		

5. AdwCleaner will now prompt you to **save any open files or documents,** as the program will need to reboot the computer. Please do so and then click on the **OK** button.

e Tools He	p.				
	4				
-01	YO L				_
-0			eo	ne	r
1					•
Pending. Please	uncheck elements you don't	want to remove.			Ĩ
Actions				Other	
200			3		hata
- Adv	Cleaner - Closing program	ns *	-		iore
Results	All are array will be	a shared in andersta some		Income	
🗼 Fe	of the infections. Pl	ease save any work in pr	ogress and then clicl	k [OK]	(A. (A)
Path			_	OK	
Path					
Path				- Chy	
Path C: C: C: C: C:	m Files (v86)) TirkyNetwork				

# **STEP 4: Remove ANY toolbar browser hijacker with Junkware Removal Tool**

Junkware Removal Tool is a powerful utility, which will remove ANY toolbar redirect from Internet Explorer, Firefox or Google Chrome.

- 1. You can download the **Junkware Removal Tool utility** from the below link: <u>JUNKWARE REMOVAL TOOL DOWNLOAD LINK</u> (This link will automatically download the Junkware Removal Tool utility on your computer)
- 2. Once Junkware Removal Tool has finished downloading, please **double-click on the JRT.exe** icon as seen below.



If Windows prompts you as to whether or not you wish to run Junkware Removal Tool, please allow it to run.

3. Junkware Removal Tool will now start, and at the Command Prompt, you'll need to *press any key* to perform a scan for the toolbar hijacker.



Please be patient as this can take a while to complete (up to 10 minutes) depending on your system's specifications.

4. When the scan Junkware Removal Tool will be completed, this utility will display a log with the malicious files and registry keys that were removed from your computer.

JRT - Notepad	
File Edit Format View Help	
Junkware Removal Tool (JRT) by Thisisu Version: 4.9.4 (05.06.2013:1) OS: Windows 7 Ultimate x86 Ran by MalwareTips on Tue 06/04/2013 at 17:35:34.55	
~~ Services	E
Registry Values	Y
Successfully repaired: [Registry Value] HKEY_CURRENT_USER\Softward Successfully repaired: [Registry Value] HKEY_USERS\.DEFAULT\Softward Successfully repaired: [Registry Value] HKEY_USERS\S-1-5-18\Softward Successfully repaired: [Registry Value] HKEY_USERS\S-1-5-19\Softward Successfully repaired: [Registry Value] HKEY_USERS\S-1-5-20\Softward Successfully repaired: [Registry Value] HKEY_USERS\S-1-5-20\Softward Successfully repaired: [Registry Value] HKEY_USERS\S-1-5-20\Softward Successfully repaired: [Registry Value] HKEY_USERS\S-1-5-21-132734	e\Microsoft\Internet Explorer\Main\\Start Page are\Microsoft\Internet Explorer\Main\\Start Page are\Microsoft\Internet Explorer\Main\\Start Page are\Microsoft\Internet Explorer\Main\\Start Page are\Microsoft\Internet Explorer\Main\\Start Page 59714-3033071532-1096447129-1000\Software\Microsof
Registry Keys	
Successfully deleted: [Registry Key] HKEY_CURRENT_USER\Software\c Successfully deleted: [Registry Key] HKEY_LOCAL_MACHINE\Software\s Successfully deleted: [Registry Key] HKEY_CURRENT_USER\Software\s Successfully deleted: [Registry Key] HKEY_CURRENT_USER\Software\A Successfully deleted: [Registry Key] HKEY_CURRENT_USER\Software\A	onduit conduit tartsearch opDataLow\Software\smartbar opDataLow\sprotector
Files	
e III.	

### **STEP 5: Remove Any Toolbar virus with Malwarebytes Anti-Malware FREE**

Malwarebytes Anti-Malware Free uses industry-leading technology to detect and remove all traces of malware, including worms, Trojans, rootkits, rogues, dialers, spyware, and more. It is important to note that Malwarebytes Anti-Malware works well and should run alongside antivirus software without conflicts.

- 1. You can download **download Malwarebytes Anti-Malware** from the below link. <u>MALWAREBYTES ANTI-MALWARE DOWNLOAD LINK</u> (*This link will open a new web page from where you can download Malwarebytes Anti-Malware Free*)
- 2. Once downloaded, close all programs, then double-click on the icon on your desktop named "*mbam-setup-consumer-2.00.xx*" to start the installation of Malwarebytes Anti-Malware.



You may be presented with a User Account Control dialog asking you if you want to run this file. If this happens, you should click "*Yes*" to continue with the installation.

3. When the installation begins, you will see the *Malwarebytes Anti-Malware Setup Wizard* which will guide you through the installation process.



To install Malwarebytes Anti-Malware on your machine, keep following the prompts by

clicking the "Next" button.



4. Once installed, Malwarebytes Anti-Malware will automatically start and you will see a message stating that you should update the program, and that a scan has never been run on your system. To start a system scan you can click on the "**Fix Now**" button.

ANTI-MALWARE		
A scan has ne	ver been run on your s	ystem Fix Now »
License:	🖌 Malwarebytes Anti-Malware Trial	Buy Premum +
Database Version:	A v2013.06.10.06	Update Now +
Scan Progress:	✓ Next scheduled scan: 2/28/2014 3:3	2:52 AM
Real-Time Protection:	✓ Malware and Malicious Website Protect	tion enabled Brd Free Trai -
Malwarebytes Secure I The name you trust to prot backs up your files. And it's that guards your files against test drive today. Learn Mor	tackup ct your computer now he only online backup malware. Take It for a Last Sca	Scan Now »
		Malwarebytes Anti-Malware
		Databases Out of Date
		Your database is out of date. It is important to keep protected by

Alternatively, you can click on the "Scan" tab and select "Threat Scan", then click on the

#### "Scan Now" button.

Malwarebytes Anti-Malware (Trial) 2.00.0.050	4	_				_ 0 ×
Malwarebytes ANTI-MALWARE	Dashboard	😳 Scan	🔅 Settings	Q History	Activate	Boy Premium
Select a Scan The scanner can find and remove	to Perform makdous software presen	) It on your system.	Select the type of sca	in you wish to run and cli	dk "Scan Now".	
Gur most capable, comprehensive	escan type. It looks in all t	the places malware	is known to hide.			
O Custom Scan     Allows you to customize where an	d what you want to scan.					
O J Hyper Scan Quickly checks your system for ac	tive threats. If anything a	s found, we recom	mend running a Threa	t Scan afterward.		
Last Updated: 4 minutes ago   Last Scan: 4 minute	es ago				Scan N	ow »

5. Malwarebytes Anti-Malware will now check for updates, and if there are any, you will need to click on the "**Update Now**" button.

Malwarebytes Anti-Malware (Trial) 2.00.0.0	504					×
	Dashboard	💮 Scan	🔅 Settings	C History	Activate	Buy Premium
Updates are ava In order to detect and quarants the update process.	ilable ne the most recent threats	it's recommended t	o perform updates vin	enever they're available.	Citck "Update Nov	/* below to begin
Updates are available. Cl	ick 'Update Now' to	download upd	ates.			
Current Software: 2.00.0.0504						
Ourrent Database: v2013.06, 10.06						
Cancel Scan				Skip	Update	Update Now

6. Malwarebytes Anti-Malware will now start scanning your computer for the pop-up virus. When Malwarebytes Anti-Malware is scanning it will look like the image below.

Malwarebytes Anti-Malware (Trial) 2.00.	0.0504					_ 0 <mark>. X</mark>
Malwarebytes ANTI-MALWARE	Dashboard	🕄 Scan	🔅 Settings	C History	Activate	Buy Premium
🗿 Threat Scar	ı			Pau	se Scan	Cancel Scan
<ul> <li>Pre-scan Operations: Done</li> <li>Memory Objects: Done</li> <li>Starbup Objects: Done</li> <li>Registry Objects: Done</li> <li>Filesystem Objects: Working Heuristic Analysis: Pending</li> </ul>	Scanner Progress: 294 Objects Scanned: 294 Detected Objects: 36 Time Elapsed: 00:1 Ourrently Scanning: C: ()	63 <u>Review Detecter</u> 01:08 WINDOWS (SYSTEM3	i Items » 2'(netevent. dl			
Malware can Malware dodges (and du machine. But malware ca installation.	t dodge Malwa dra, dips, dives and . dodges) i't fool Malwarebytes. The pr	i <b>rebytes Ch</b> ) arti-makware's atte oprietar y Makwareby	n <b>ameleon</b> mpts to find it. It can i rtes Chameleon techni	even block the installatio ology makes it so even t	in of anti-malwar he smartest malv	e on an infected nare can't block its Learn more .»

7. When the scan has completed, you will now be presented with a screen showing you the malware infections that Malwarebytes' Anti-Malware has detected. To remove the malicious programs that Malwarebytes Anti-malware has found, click on the "**Quarantine All**" button, and then click on the "**Apply Now**" button.

Choose an a	ction for the de	etected items!		o.		
Detected Item	Туре	Action	100	Location		
ojan.Zbot	File	Quarantine		C: \Users \MalwareTips \Ap	opData\Roaming	\Xaotko\yyf.exe
rojan.Zbot	Registry Value	Quarantine	*	HKU\S-1-5-21-17589910	82-695353234-2	2857450141-1000-{ED1FC
ojan, Zbot	Process	Quarantine	*	C; \Users\MalwareTips\Ap	opData\Roaming	\Xaotko\yyf.exe
ackdoor.Agent.DCRSAGen	File	Quarantine	*	C:\Users\MalwareTips\D	ownloads\2014-0	02-25\2014-02-25\gg.exe
ackdoor.Agent.DCRSAGen	Process	Quarantine	*	C:\Users\MalwareTips\Do	ownloads\2014-0	02-25\2014-02-25\gg.exe
ackdoor.Agent.DCRSAGen	Process	Quarantine		C:\Users\MalwareTips\Do	ownloads\2014-(	02-25\2014-02-25\gg.exe
rus Slunin	File	Quarantine		C-11 Isers/MalwareTins/&r	onData\Roaminn	\Tostall\bkrmd.eve
Quarantine All						Cancel

- Please note that the infections found may be different than what is shown in the image.
- 8. Malwarebytes Anti-Malware will now quarantine all the malicious files and registry keys that it has found. When removing the files, Malwarebytes Anti-Malware may require a reboot in order to remove some of them. If it displays a message stating that it needs to reboot your computer, please allow it to do so.



After your computer will restart, you should open Malwarebytes Anti-Malware and perform another "Threat Scan" scan to verify that there are no remaining threats

# **STEP 6: Double-check for the Toolbar infection with HitmanPro**

HitmanPro is a second opinion scanner, designed to rescue your computer from malware (viruses, trojans, rootkits, etc.) that have infected your computer despite all the security measures you have taken (such as anti virus software, firewalls, etc.). HitmanPro is designed to work alongside existing security programs without any conflicts. It scans the computer quickly (less than 5 minutes) and does not slow down the computer.

- 1. You can download **HitmanPro** from the below link: <u>HITMANPRO DOWNLOAD LINK</u> (*This link will open a new web page from where you can download HitmanPro*)
- 2. Double-click on the file named "**HitmanPro.exe**" (for 32-bit versions of Windows) or "**HitmanPro\_x64.exe**" (for 64-bit versions of Windows). When the program starts you will be presented with the start screen as shown below.



Click on the "Next" button, to install HitmanPro on your computer.

(ep (el a)	
Would you like to store a cop	of the HitmanPro program file on this computer?
Yes, create a copy of Hitr	nanPro so I can regularly scan this computer (recommended)
Automatically scan	the computer daily during startup
Create a shortcut o	the desktop
Create shortcuts in	the Start menu
No, I only want to perfor	n a one-time scan to check this computer
Registration	
Registration E-mail Address:	
Registration E-mail Address: Confirm E-mail Address:	
Registration E-mail Address: Confirm E-mail Address:	Please e-mail me important product notifications and opportunities to save on enhancements to my online security

3. HitmanPro will now begin to scan your computer for any malicious files that may be on your machine.

Iassifying (71%)	and the second	1m 24
-\Windows\SysWOW64\d3dx10_35.dll		
fiv_en_1.exe C\Users\MalwareTips\Desktop\	😵 Riskware	Quarantine 👻 🔺
LocalHWUntwhaOX.exe C:\Users\MalwareTips\Downloads\xalwdxc\	😵 Trojan 🗟	Delete 👻 🗍
LocaltciyFNkbjT.exe C\Users\MalwareTips\Downloads\xalwdxc\	😵 Malware	Quarantine 👻
fiv_en_1.exe C\Users\MalwareTips\Downloads\	😵 Riskware	Quarantine 👻
bot (3).exe C:\Users\MalwareTips\Downloads\xalwdxc\	😵 Trojan	Delete 💌
cd.exe C:\Users\MalwareTips\Downloads\xalwdxc\	😵 Trojan	Delete 🕶
kl.exe C:\Users\MalwareTips\DownToads\xalwdxc\	😵 Trojan	Quarantine 👻
exe-gpi.Scr C:\Users\MalwareTips\Downloads\xalwdxc\	😵 Trojan	Delete 🛩
bot (2).exe	😵 Trojan	Delete 🕶 👻
dentified Threats: 55 (Traces: 61)		61 Item

4. When it has finished it will display a list of all the malware that the program found as shown in the image below. Click on the "**Next**" button, to remove any virus that has been

#### found.

CAN results falicious software was detected. Close all applications and c ertain programs may terminate unexpectedly.	lick Next to remove t	he malicious softw	1m 52 are. During removal,
flv-player.exe C:\Users\MalwareTips\Desktop\	8	Riskware	Quarantine 👻 🍝
Re-Markable_2040-2083.exe C:\Users\MahwareTips\Desktop\	8	Riskware	Quarantine 🔫
Re-Markable_2040-2083.exe C\Users\MalwareTips\Downloads\	8	Riskware	Quarantine 👻
fiv_en_1.exe C^Users\MaiwareTips\Downloads\	8	Riskware	Quarantine 👻
fix_even.exe C\Users\MahwareTips\Downloads\	8	Riskware	Quarantine 🔫
PricePeep.exe C:\Users\MatwareTips\Downloads\	8	Riskware	Delete 🔻
bot (3).exe C:\Users\MaiwareTips\Downloads\xalwdxc\	8	Trojan	Delete 👻
cd.exe C\Users\MalwareTips\Downloads\xalwdxc\	8	Trojan	Delete 🕶
kl.exe	8	Trojan	Quarantine 👻 🔫
lentified Threats: 107 (Traces: 114)			114 Item
Buy Now Save Log		Next	Close

5. Click on the "Activate free license" button to begin the free 30 days trial, and remove all the malicious files from your computer.

HitmanPro 3.7.9 - Build 21.	2 (64-bit)			
Product Activation				
Activate your copy of Hitm	anPro to remove malicious softwa	re.		
Please enter the product ke XXXXXX-XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	y that you received when you purc KX. Activation will register the prod	hased HitmanPro in the fiel luct key to this computer.	d below in format	
Product Key:	1		Activate	
	I do not have a product key			
License Information	0			
A HitmanPro is not a	tivated.			
Buy Now			Next	Cancel