Removing "Crapware" (aka Potentially Unwanted Programs (PUPs))

Lately the biggest problem I've been seeing on member's Windows computers is not computer viruses – it's 'Crapware.' The software industry has to be a bit more politically correct, so they call these 'Potentially Unwanted Programs' or PUPs but it's still crap. <grin> The term PUP was coined by McAfee because the writers of this crap objected to their finely crafted programs being called 'Spyware.' LOL!

I am talking about those programs that sneak onto your computer and make changes that you probably don't want. Things like:

- Changing your browser home page to somewhere else so that page can sell more advertising.
- Changing your search engine to something else so that search engine can sell more advertising.
- Adding toolbars so that the vendor can sell more advertising that's always right in front of you.
- Adding a 'Browser Helper Object' that will <u>replaces</u> ads on a webpage with their ads.
- Claiming 'Free' download and 'Free' install of Windows utilities but then ask you to pay for the program to do anything useful.

Note the common factors – it's not about you; it's about 'them' and whether 'they' can get money out of you or even more indirectly, get money out of other business just to show you yet more advertising. They really don't care if they mess up your computer only if they can make money from somebody.

Like I said, "crap." And because this is just between you and me and the Internet, I'll name some names: PC Optimizer Pro, Systweak, Trymedia, Advanced System Protector, RegClean Pro, MyPC Backup, MyWebSearch, the many flavors of Conduit, 24x7 Help, Site Ranker, Driver Update, Babylon and on and one. Here's a link to a short list of 233 PUPs: <u>http://www.enigmasoftware.com/threat-</u> <u>database/potentially-unwanted-programs</u>. I'm sure there are more and more popping up every day. There's money to be made!

It's best not to get this stuff installed in the first place, but it's hard to avoid. A program like ImgBurn (a good program user to create and write CD and DVD images) is bundled with no less that nine extra, 'recommended' crapware programs when downloaded from CNet. (aka Download.com) There are ways avoid crap installations, but this paper is more about recovering after this stuff is installed.

Ok, I'll give. <grin> Here are the easiest ways to avoid crapware:

First, never accept the 'express', 'recommended', or 'easy' installation methods for software; always select the 'custom' or 'advanced' methods. *Read* the prompts carefully, sometimes the right answer is no, sometimes it's yes, sometimes it's decline. They will try to trick you, but they have to tell the truth. Say no to anything not directly related to the program you want.

Second, if the program you want is on Ninite – install it from there. The Ninite installer is great and avoids all crapware and add-ons, plus if you save the Ninite installer it will update all the programs easily.

Third, you probably don't need that 'Free' program advertised on that webpage. And it's probably not free. Trust recommendations from the computer club or independent third-party reviewers. We like 'Ask Bob' and 'Ask Leo' - <u>http://askbobrankin.com/</u> and <u>http://askleo.com/</u>.

Because this stuff is not strictly speaking 'Malware', it can be uninstalled. The Windows add/remove program applet *should* uninstall those programs which you don't want. And you can reset browsers for home pages, search engines and toolbars. But remember these guys are tricky, for example, after replacing your search page, Conduit installs a "Search Protection" program to make it hard for you to change it back!

For those people that just want advice on what to keep and what to uninstall, the free program "Should I Remove It" (<u>http://www.shouldiremoveit.com/</u>) is a good choice. This, after being installed and run, reviews all the other programs installed on your computer and provides, 1) a community consensus for removal (Red/Amber/Green ratings), 2) a link to tell you what is program does, and 3) an uninstall button. Even if you don't install the program, the SIRT website is a good resource for looking up suspect programs. For example, here is a link for the 'InBox Toolbar', <u>http://www.shouldiremoveit.com/Inbox-Toolbar-14053-program.aspx</u> . (p.s., this thing has nothing to do with email and everything to do with advertising.)

Now to the meat of this note: I have recently found two programs, "AdwCleaner" and "JRT" which are designed to help remove most crapware. Paired with our old, but recently updated "MalwareBytes," these three programs do a great job in removing the stuff you really don't want on your computer. This is a step-by-step instruction of how to use these tools.

Step 0: Create a system restore point. (optional)

The System Restore feature in Windows keeps snapshots of programs and system settings. In the case of difficulties, System Restore can return your computer to the state it was as of sometime in the past. You should create a new system restore point in case something goes badly wrong in the following steps.

For Windows Vista, 7, and 8 search for "Point" to find the "Create a Restore Point" command. (For Windows XP, the command is in the System Restore program under Accessories/System Tools.)

Create one by clicking the Create Button

Step 1: Run AdwCleaner

The hardest part of AdwCleaner is finding and downloading it. Not because of any inherent difficultly, but because it gets updated frequently and it's in French. However, the website "Bleeping computer" keeps a live copy of the version of AdwCleaner in English. Click this link to the Bleeping Computer download: <u>http://www.bleepingcomputer.com/download/adwcleaner/</u>

AdwCleaner Download ×			
← → C fi D www.bleepingcomputer.com	/download/adwcleaner/		승 =
Apps () Cleveland PC Users TN WHS 2011 Help B	te 🎬 BaenCDs 🔃 Bloatware 🤷 Win7 and SSDs 🕒 APCUG Virt	ual 📢 iPod Copy 📑 Outlook 2010 Search 🏢 NASCAR.COM 🕺	The News Journal » 🗀 Other bookmarks
Welcome Guest (Log In Create Account) Home > Downloade > Windows > Security > Security	pringcomputer.com me forums Downloads Tetorialis Startup Li y Utilities > AdvcCeanor 3.0.2.3	st] Virus Removal Uninstal List File Database Gossary	- New Member? Join for free, Welcome Cale Chil Help Search RS
Platforms	AdwCleaner 3.0.2.3 Download	8+1 204 ELike 3.5k Tweet 172	Most Downloaded in Windows
Windows Mac Linux	Free Malware Removal (Recommended) Remove Malwar	e In 2 Minutes. Free Download	DOWNLOADS FOR LAST WEEK 1. ComboFix 252,613 2. AdwCleaner 222,535
Windows Categories	Sponsored Ad	vertisement	3. RKill 46,494
Security Educational Networking	Author: Xplode License: Free Concreting Windows XP/Vista/7/8	Download Now @BleepingComputer	4. Junkware Removal Tool 40,154 5. TDSSKiller 23,356
Photos & Images	System: 32-Bit and 64-Bit	Author's Site	Search Downloads
Audio	Version: 3.0.2.3 File Size: 1.36 MBs		
Development	Downloads: 8,622,135		Search
EVENT LOG CONSOLIDATOR	201 (#3.5k) S ⁻¹ (Item) R AdwCleaner	172 11 Trott in Stare	MASTER BIG DATA WITH SSDs.

Note the big green "Free Download" button – that is *Not* the right download! (That's crap!)

System Properties			×					
Computer Name Ha	rdware Advanced	System Protection	Remote					
Use system restore pre-	protection to undo u rious versions of files	inwanted system cha . What is system prot	nges and ection?					
System Restore								
You can undo syste your computer to a	You can undo system changes by reverting System Restore							
Protection Settings								
Available Drives		Protection						
🃗 ImageBacku	p	On						
SSD-W7Ult	C:) (System)	On						
🕞 HDD-1TB (D	:)	On						
Configure restore and delete restore	Configure restore settings, manage disk space, Configure							
Create a restore p	oint right now for the		eate					
T	ОК	Cancel	Apply					

The <u>correct</u> download is the Blue button labelled "Download Now @Bleeping Computer." Click that.



Ok the download if prompted. Recommend selecting Save not Run. The filename downloaded will be "AdwCleaner.exe." If it's anything else, beware!

Since this is an executable file, some browsers may block the download. For example, Chrome indicates

ome				
ad.	7	This type of file can harm your computer. Do you want to keep AdwCleaner.exe anyway?	Кеер	Discard

Click "Keep."

An AdwCleaner advantage is it does not have to be installed, just run. After running it, nothing is left over to slow your computer down. Locate the download and double-click it. (Hint: Downloads are by default saved in the 'username\Downloads' folder.)

You will probably get two warning from Windows. Go ahead and click 'Run' and 'Yes'



Click the Left button, "J'accepte" (Accept).



The program will open. Click the 'Scan' button, then wait while the computer is scanned.

File Tools Help	File Tools Help
Adwcleøner	Adwcle o ner
Awaiting action.	Searching for files
Complete name Co	Actions Actions Image: Report Image:
	Scanning

After the scan has completed, the results will be shown. The line above the progress meter will change to "Pending ... " and the Clean button lights up.

All items found will be selected for deletion by default. I like that default! Feel free to see the items found by clicking through the various tabs.

Before clicking the "Clean" button – close all other programs. If you forget they will be closed automatically. (I had to redo this page because I forgot. O)

Your last chance to close programs is now:



-	Adwcle&ner
ending. Pl	ease uncheck elements you don't want to remove.
	Scan Cean Report Uninstal
J Folde	rrs 🕐 Files 🐧 Shortcuts 👹 Registry 🏈 Internet Explorer 🏈 Firefox 🏈 Chrome
Key	HKLM\SOFTWARE\Classez\ApplD\(0A18A436-2A7A-49F3-A488-30538A2F6323)

All the selected (crapware) items will be removed and then your computer will be restarted. Done!

Option: Although nothing was installed, AdwCleaner does leave behind a quarantine folder and some logs. To remove these easily, just run AdwCleaner again and click the 'Uninstall' button. Or open the folder and see the names of the crap that was deleted in the log. ©

Step 2: Run JRT

JRT stands for 'Junkware Removal Tool' and it does similar things that AdwCleaner does, but in a slightly different way. It's good to use both tools as they catch different things. Also downloaded from Bleeping Computer, click this link: <u>http://www.bleepingcomputer.com/download/junkware-removal-tool/</u>



Again, click the *blue* download button, not a Green one. Save the file to your computer, then run it.



Administrator: Junkware Removal Tool by Thisisu - Version 6.1.4		JRT will then scan your
[This software is provided "as is" without] [warranty of any kind. You may use this software] [at your own risk.] [Click the [X] in the top-right corner of this window] [if you wish to exit. Otherwise,]	·	computer for junk. When the JRT log appears, is done:
Press any key to continue		ii JRT.txt - Notepad
Greating a registry backup Checking Startup Checking Modules Checking Processes Checking Samutae		Junkware Removal Tool (JRT) by Thisisu Version: 6.1.4 (04.06.2014:1) OS: Windows 7 Ultimate x64
Checking Files Checking Folders Checking Registry Checking Internet Explorer Checking Mozilla FireFox Checking Gozalla Cheme		Kan by NewKob on Sun U4/13/2014 at 13:41:05.78
Clearing Event Viewer Logs Checking Shortcuts	-	~~~ Services

Feel free to review the log for a list of things removed, the log is saved on the desktop as a Notebook file. Delete the log when done unless you have a specific reason to save it. Done!

Step 3: MalwareBytes

MalwareBytes is our go to tool for a second opinion on computer viruses. It's also very good for crapware, which it calls the politically correct "PUPs." <u>https://www.malwarebytes.org/</u> is the site, but I think it's easier to download, install and update from Ninite, <u>http://ninite.com/</u> :

Ninita Install or Line						
← → C fi []	ninite.com		-			= 12
Apps 🕥 Cleveland F	PC Users TN WHS 2011 He	elp Byte 📓 BaenCE)s 🔃 Bloatware 🥶 Win7	and SSDs 🕒 APCUG Vir	tual 🕤 iPod Copy	» 🧰 Other bookmarks
Ninite "	vindows linux pro upd	ater			help	feedback sign in
Install and	d Update All Your	Programs at Or	nce Alwa	ys Up-to-date	Trusted by	Millions
Ninite			You do Our bot	n't have to watch for upd s do that. Here's what's	ates. We install and up new: programs each da	date over 500,000 ly for millions of
Installing Pidgi	n		KeePa: 4 hours	ss 2 updated to 2.26. ago	home users and <u>1</u> subscribers like N Medical School, a	<u>linite Pro</u> IASA, Harvard ind Tupperware.
			foobar2	000 updated to 1.3.2.	The <u>press</u> likes u	s too:
Hide details Application Firefox	Status Skipped (up to dat	Write feedback Car	AVG u Thursda	at 8:40 am pdated to 14.0.4569. ay at 5:49 pm	"I'll bet the service hours" PCWorld	saved me a couple
Skype VLC Pidgin Messenger	OK OK Installing Waiting to install	-	Spotify Thursda	updated to 0.9.8.296. ay at 6:57 am	"Ninite.com frees The Christian So	up your day" sience Monitor
iTunes LibreOffice	Downloading Waiting to downloa	ad	LibreOf Thursda	fice updated to 4.2.3. ay at 6:50 am	"This post can be Ninite works exac Lifehacker	fairly short because tly as advertised."
No toolbars. N	o clicking next. Just pick	your apps and click Get	installer.	d run it 3.	Run it again later	
You can learn over it.	more about a program by	hovering Ninite in clicking	stalls apps for you in the b next. We say NO to toolba	ackground. No You rrs or other junk. vers	ir installer will up ote apps t sions. If something to up-to-d	othe latest ate we'll skip it.
Web Browsers	Messaging	Media	Runtimes	Imaging	Documents	Security
Chrome	U SSkype	🗆 👩 iTunes	🔲 🔬 Java	U 🛃 Paint.NET	U SopenOffice	Essentials
UOpera Chromiun Eirofox	n 🔲 💇 Pidgin		NEI Silvadiabt	Picasa	Keader GumatraPDE	Avast
	Google Talk	C KMPlaver	Air	With the second seco	Virginia Sumanan Di Virginia Sumanan Di Vir	Malwarebytes
File Sharing	Construction (Construction)		Shockwave	🗆 😻 XnView	CutePDF	Ad-Aware
🔲 🌚 qBittorrent	🗆 🐁 Trillian	foobar2000		🗆 🏶 Inkscape	LibreOffice	Spybot 2
🗆 🐔 eMule	🗆 😤 AIM	🗆 🔗 Winamp	Online Storage	CastStone 💿	PDFCreator	Avira
	WYahoo!	Audacity	🔲 💙 Dropbox	Greenshot	—	Super 🔹

Simple check any programs that you want to install or update – MalwareBytes in checked in the above screen shot. Then scroll down till you see the big green "Get Installer" button and click that:



it

The Ninite [list of programs].exe file will download to your computer, usually to the 'Downloads' folder. The advantage of the Ninite method is whether or not you already have (whatever programs you selected) installed or not, Ninite does the right thing:

- If the program(s) are not installed, Ninite installs them 'cleanly,' no add-ons, toolbars, or other junk.
- If the program(s) are installed but not updated, Ninite updates to the most current version.
- If the program(s) are installed and updated to the most current version, Ninite skips them.

When Ninite is run, the programs selected will be installed or updated and icon(s) be placed on your desktop. Double-click the downloaded Ninite installer and click Yes to the UAC prompt:



(Hint: Save the Ninite installer, you can run it at any time in the future to simply update your programs.)

Now we can run Malwarebytes, double-click the icon:



\mathcal{D}	Malwaret	bytes An	ti-Malware	(Free)		
	License:		8 Malwarebytes Anti	-Malware (Free)	Buy Pr	enium +
	Database Version:		✔ v2014.04.13.05		Updat	e Now +
	Scan Progress:	2	Not Running			
	Real-Time Protect	ion:	🕄 Available with Maile	varebytes Anti-Malware Premiu	m Start P	ee Trial +
rebytes A Malwa	inti-Malware (Free) 2.0. srobytos FI-MALWARE	1.1004	board 🚯 Scan	🏶 Settings 📿 Histo	ory Activate	Buy Premi
Malwa	unti-Malware (Free) 2.0. prebytos FI-MALWARE Threat Sca	1.1004 : ① Dash	iboard 💽 Scan	🇱 Settings 📿 Histo	ory Activate Pause Scan C	Buy Prem

Malwarebytes will open.

For those familiar with MalwareBytes, it may look different than you remember as it has been recently updated to version 2.

If the threat databases are noted as being old, click the update link.

When ready, click the 'Scan Now' button.

The scan checks six areas of the computer.

Let it complete, on most computer this should not take over 10 minutes.

Here's an example of what it will look like after the scan is complete and malware (or PUPs) are found:

NO.				Export Log 👻 Copy to Clipboa	rd	
					-	
Choose an a	ction for the d	etected items!				
Detected Item	Туре	Action		Location		
Trojan.Zbot	File	Quarantine	٣	C:\Users\MalwareTips\AppData\Roaming\Xaotko\yyf.exe	H	
Trojan.Zbot	Registry Value	Quarantine	٣	HKU\S-1-5-21-1758991082-695353234-2857450141-1000-{ED1PC765-E35E-4C3D-8	-	
Trojan, Zbot	Process	Quarantine	*	C: Users WalwareTips \AppData \Roaming \Xaotko \Vyyf.exe		
Backdoor.Agent.DCRSAGen	File	Quarantine	٣	C: Users (MalwareTips (Downloads \2014-02-25\2014-02-25\gg.exe		
Backdoor.Agent.DCRSAGen	Process	Quarantine	Ŧ	C: \Users\MalwareTips\Downloads\2014-02-25\2014-02-25\gg.exe		
Backdoor.Agent.DCRSAGen	Process	Quarantine	*	C: \Users\MalwareTips\Downloads\2014-02-25\2014-02-25\gg.exe		
Virue Skanin	File	Ouserantine	*	C-11 Isers/MalwareTins/JannData/Roaminn/Tristall/Inkrmid eve	K	
Quarantine All				Cancel Apply Action	s	
						J
				Mahumahidan Anti Mahuma		171

I recommend reviewing the list and setting the action to 'Quarantine' for all found items, regardless of the detected item. If you specifically see something that you know is something you want to keep, you can set the action to ignore – but I find this very rare.

Click 'Apply Actions' and watch the malware disappear. You may have to restart the computer afterward to make sure all the junk is deleted.

You can find a Malwarebytes guide here: <u>http://www.malwarebytes.org/support/guides/mbam/</u>

Last Step – Reset your Browser

Crapware often also makes configuration changes to browsers, and unfortunately, changed Home Pages and Search Engines may not be restored when the crapware is removed. 'Resetting' your browser will remove all of these customizations. This is how to do that:

Internet Explorer:

Click the gear just under the [X] box on the upper right.





Select Internet Options - Click on the 'Advanced' tab – Click Reset – and finally the Reset button.

FireFox

Click the arrow next to 'Firefox,' then Help, and then Troubleshooting Information. (If the menu is shown, select Help, then Troubleshooting Information.)



Finally, click the 'Reset Firefox' button.

Chrome

Click the settings icon (3 lines) just under the [X] box on the upper right

Q & E	Search	
New tab Ctrl+T New window Ctrl+N New incognito window Ctrl+Shift+N Bookmarks ▶ Recent Tabs ▶	Set which search engine is used when searching from the Google Manage search engines	
Edit Cut Copy Paste Zoom - 90% + [] [] Save page as Ctrl+S Find Ctrl+F Print Ctrl+P	Users You are currently the only Google Chrome user. Add new user Delete this user Import bookm	
Tools ▶ History Ctrl+H Downloads Ctrl+J Sign in the norme Stettings About Google Chrome	Default browser Make Google Chrome the default browser Google Chrome is not currently your default browser.	Reset browser settings Restore browser settings to their original defaults. Reset browser settings
Help Exit Ctrl+Shift+Q	Show advanced settings	Hide advanced settings

Scroll to the bottom of the Settings Page, click Show Advanced Settings, scroll to the bottom again, and click on the 'Reset browser settings' button

ſ	Reset browser settings	×
ic	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 up in all tabs It will also clear other temporary and cached data, such as cookies, content of site data.	
lo	Learn more Reset Cancel	
e	${f S}$ Help make Google Chrome better by reporting the current settings ${\ensuremath{\otimes}}$	

Read the prompt and click 'Reset'

This is by no means a comprehensive guide to Malware or 'Crap' cleaning. There are computer viruses that are expressly written to hide from these tools. But the use of these tools will go a long way to help you keep your Windows running neat and clean.

- Bob Bloom, Newark Senior Center Computer Club, ask@nscseniorsurfers.com

QC