

How to easily clean an infected computer (Malware Removal Guide)

Malware, short for malicious (or malevolent) software, is software used or programmed by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. ‘Malware’ is a general term used to refer to a variety of forms of hostile or intrusive software.

Malware includes computer viruses, ransomware, worms, trojan horses, rootkits, keyloggers, dialers, spyware, adware, malicious BHOs, rogue security software and other malicious programs; the majority of active malware threats are usually worms or trojans rather than viruses.

It’s not always easy to tell if your computer was compromised or not, because these days cybercriminals are going to great lengths to hide their code and conceal what their programs are doing on an infected computer.

It’s very difficult to provide a list of characteristic symptoms of a infected computer because the same symptoms can also be caused by hardware incompatibilities or system instability, however here are just a few examples that may suggest that your PC has been compromised :

- You may receive the error “Internet Explorer could not display the page” when attempting to access certain websites
- Your web browser (e.g., Microsoft Internet Explorer, Mozilla Firefox, Google Chrome) freezes, hangs or is unresponsive
- Your web browser’s default homepage is changed
- Access to security related websites is blocked
- You get redirected to web pages other than the one you intended to go to
- You receive numerous web-browser popup messages
- Strange or unexpected toolbars appear at the top of your web browser
- Your computer runs slower than usual
- Your computer freezes, hangs or is unresponsive
- There are new icons on your desktop that you do not recognize
- Your computer restarts by itself (but not a restart caused by Windows Updates)
- You see unusual error messages (e.g., messages saying there are missing or corrupt files folders)
- You are unable to access the Control Panel, Task Manager, Registry Editor or Command Prompt.

This article is a comprehensive guide, which will remove most of malware infections that may reside on your computer. And if you are experiencing any of the above symptoms, then we strongly advise you follow this guide to check and remove any infection that you might have on your computer.

How to remove viruses, ransomware, worms, trojan horses, rootkits, keyloggers, dialers, spyware, adware, malicious BHOs, rogue security software and other malicious programs

OPTIONAL: Some forms of malware will not allow you to start some of the below utilities and on-demand scanners, while running Windows in Normal mode. If this happens, we recommend that you start your computer in Start your computer in Safe Mode with Networking, and try from there to perform the scan.

We recommend that you first try to run the below scans while your computer is in Normal mode, and only if you are experiencing issues, should you try to start the computer in Safe Mode with Networking.

To start your computer Start your computer in Safe Mode with Networking, you can follow the below steps:

1. Remove all floppy disks, CDs, and DVDs from your computer, and then **restart your computer.**
2. **If you are using Windows XP, Vista or 7 press and hold the F8 key as your computer restarts.** Please keep in mind that you need to press the F8 key **before the Windows start-up logo appears.**

Note: With some computers, if you press and hold a key as the computer is booting you will get a stuck key message. If this occurs, instead of pressing and holding the “F8 key”, **tap the “F8 key” continuously** until you get the *Advanced Boot Options* screen. If you are using Windows 8, press the **Windows key + C**, and then click **Settings**. Click **Power**, **hold down Shift** on your keyboard and click **Restart**, then click on **Troubleshoot** and select **Advanced options**.

3. In the **Advanced Options** screen, select **Startup Settings**, then click on **Restart**.
4. If you are using Windows XP, Vista or 7 in the *Advanced Boot Options* screen, use the arrow keys to **highlight Safe Mode with Networking** , and then **press ENTER**.

```
Windows Advanced Options Menu
Please select an option:

Safe Mode
Safe Mode with Networking ←
Safe Mode with Command Prompt

Enable Boot Logging
Enable UGA Mode
Last Known Good Configuration (your most recent settings)
Directory Services Restore Mode (Windows domain controller)
Debugging Mode
Disable automatic restart on system failure

Start Windows Normally
Reboot

Use the up and down arrow keys to move the highlight to your
```

If you are using **Windows 8**, press **5** on your keyboard to **Enable Safe Mode with Networking**.

Windows will start in Safe Mode with Networking.

STEP 1: Remove bootkits and trojans with Combofix

In this first step, we will run a system scan with Combofix to remove any malicious software that might be installed on your system.

1. Download Combofix from any of the below links.
[COMBOFIX DOWNLOAD LINK #1](#) (This link will automatically download Combofix on your computer)
[COMBOFIX DOWNLOAD LINK #2](#) (This link will automatically download Combofix on your computer)
2. Before running this utility ,please follow the below instructions:
 - o Close any open browsers.
 - o **Temporarily disable your anti-virus**, script blocking and any anti-malware real-time protection **before performing a scan**. They can interfere with ComboFix or remove some of its embedded files which may cause “*unpredictable results*”.
 - o Combofix will disconnect your machine from the Internet as soon as it starts. Please do not attempt to re-connect your machine back to the Internet until Combofix has completely finished.
If there is no internet connection after running Combofix, then restart your computer to restore back your connection.
3. To start the Combofix scan, double-click on ComboFix.exe and then follow the prompts. You can watch the below video to see how to use Combofix:

Other important notes:

- **DO NOT** mouse-click Combofix's window while it is running. That may cause it to stall.
- If after the reboot you get errors about programs being marked for deletion then reboot, that will cure it.

STEP 2: Run RKill to terminate any malicious processes

RKill is a program that will attempt to terminate all malicious processes that are running on your machine, so that we will be able to perform the next step without being interrupted by this malicious software.

Because this utility will only stop the running process, and does not delete any files, after running it you should not reboot your computer as any malware processes that are configured to start automatically will just be started again.

1. Please **download the latest official version of RKill**. Please note that we will use a renamed version of RKILL so that malicious software won't block this utility from running.

[**RKILL DOWNLOAD LINK**](#) (This link will automatically download RKILL renamed as *iExplore.exe*)

2. Double click on **iExplore.exe** to start RKill and stop any processes associated with Luhe.Sirefef.A.



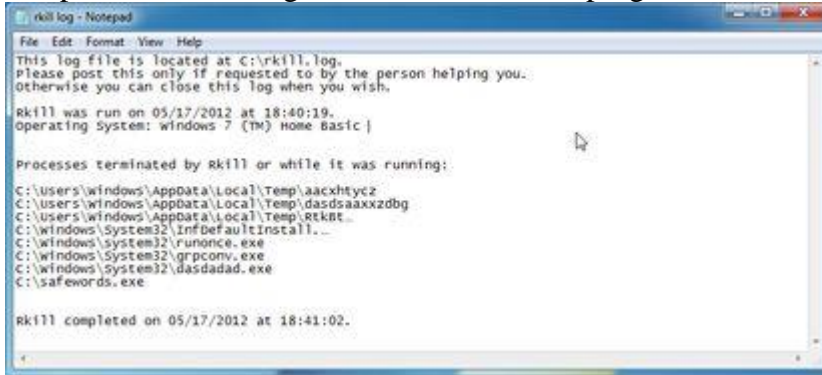
3. RKill will now start working in the background, please be patient while the program looks for any malicious process and tries to end them.

```

C:\Users\MalwareTips\Downloads\iExplore.exe
Resetting .EXE, .COM, & .BAT associations in the Windows Registry.
Performing miscellaneous checks:
* Windows Defender Disabled
[HKLM\SOFTWARE\Microsoft\Windows Defender]
"DisableAntiSpyware" = dword:00000001
* Windows Firewall Disabled
[HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile]
"EnableFirewall" = dword:00000000
Checking Windows Service Integrity:
* Windows Defender (WinDefend) is not Running.
Startup Type set to: Manual
* FontCache => %SystemRoot%\system32\svchost.exe -k LocalService {Incorrect ImagePath}
Searching for Missing Digital Signatures:

```

4. When the Rkill utility has completed its task, it will **generate a log**. Do not reboot your computer after running RKill as the malware programs will start again.



```
File Edit Format View Help
This log file is located at C:\rkill.log.
Please post this only if requested to by the person helping you.
Otherwise you can close this log when you wish.

Rkill was run on 05/17/2012 at 18:40:19.
Operating System: windows 7 (TM) Home Basic

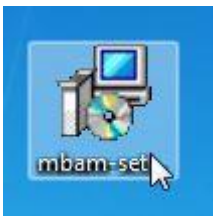
Processes terminated by Rkill or while it was running:
C:\Users\windows\AppData\Local\Temp\aacxhtycz
C:\Users\windows\AppData\Local\Temp\dasdsaaxzdbg
C:\Users\windows\AppData\Local\Temp\rekkt...
C:\windows\System32\InfDefaultInstall...
C:\windows\system32\runonce.exe
C:\windows\System32\grpconv.exe
C:\windows\System32\dasdadad.exe
C:\safewords.exe

rkill completed on 05/17/2012 at 18:41:02.
```

STEP 3: Remove Trojan Horses, rogue security software and other malicious files from your computer 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. [MALWAREBYTES ANTI-MALWARE DOWNLOAD LINK](#) (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.



3. 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.

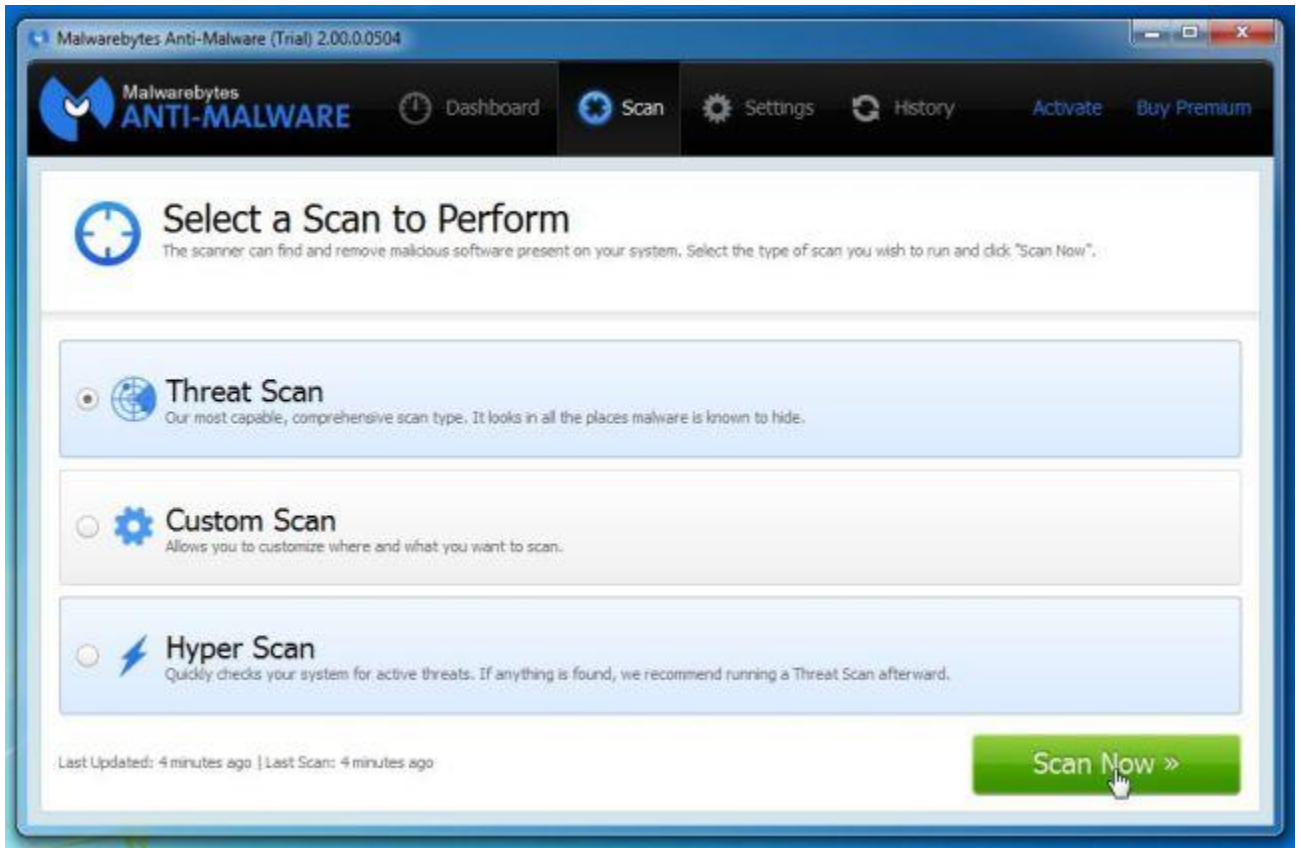


4. Once installed, Malwarebytes Anti-Malware will automatically start and you will see a message stating that you should update the program, and that a scan has never been run on your system. To start a system scan you can click on the “**Fix Now**” button.

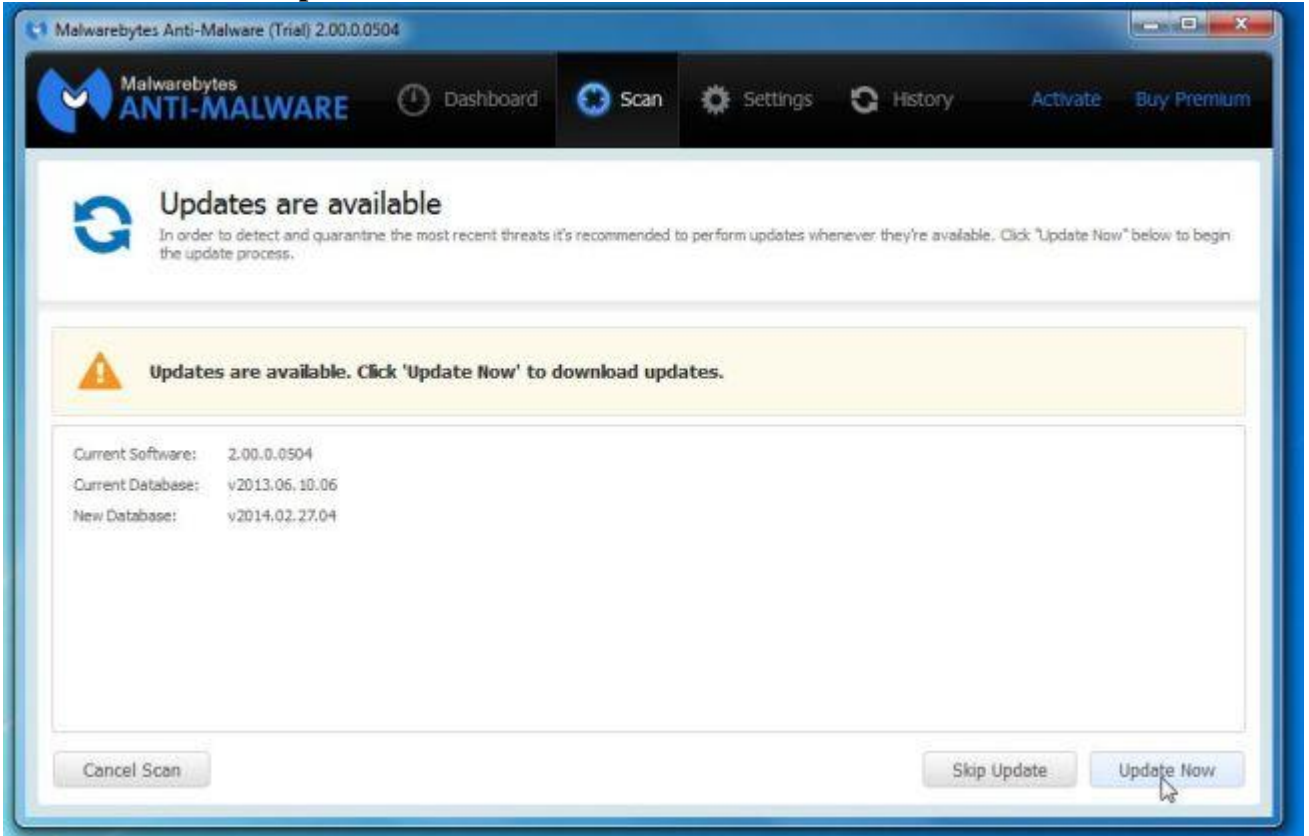


Alternatively, you can click on the “**Scan**” tab and select “*Threat Scan*“, then click on the

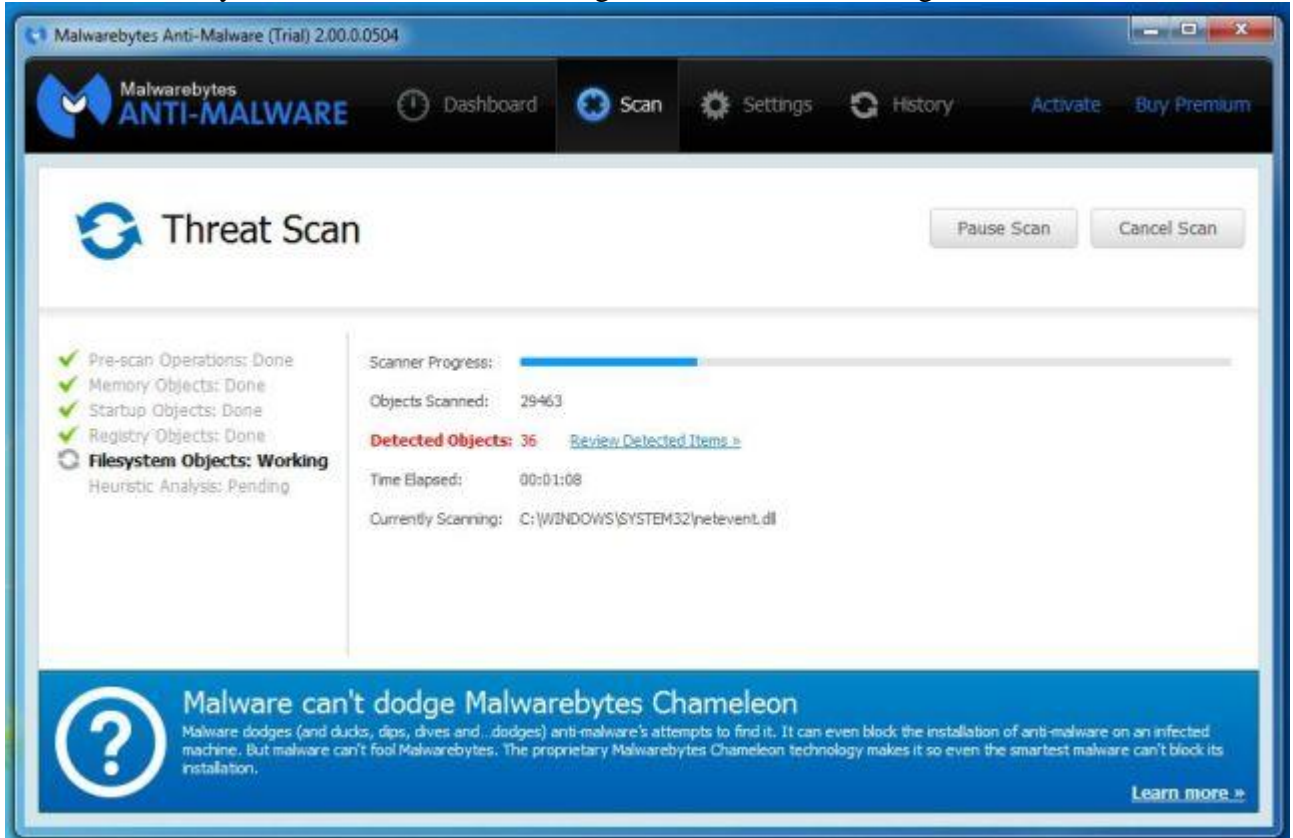
“Scan Now” button.



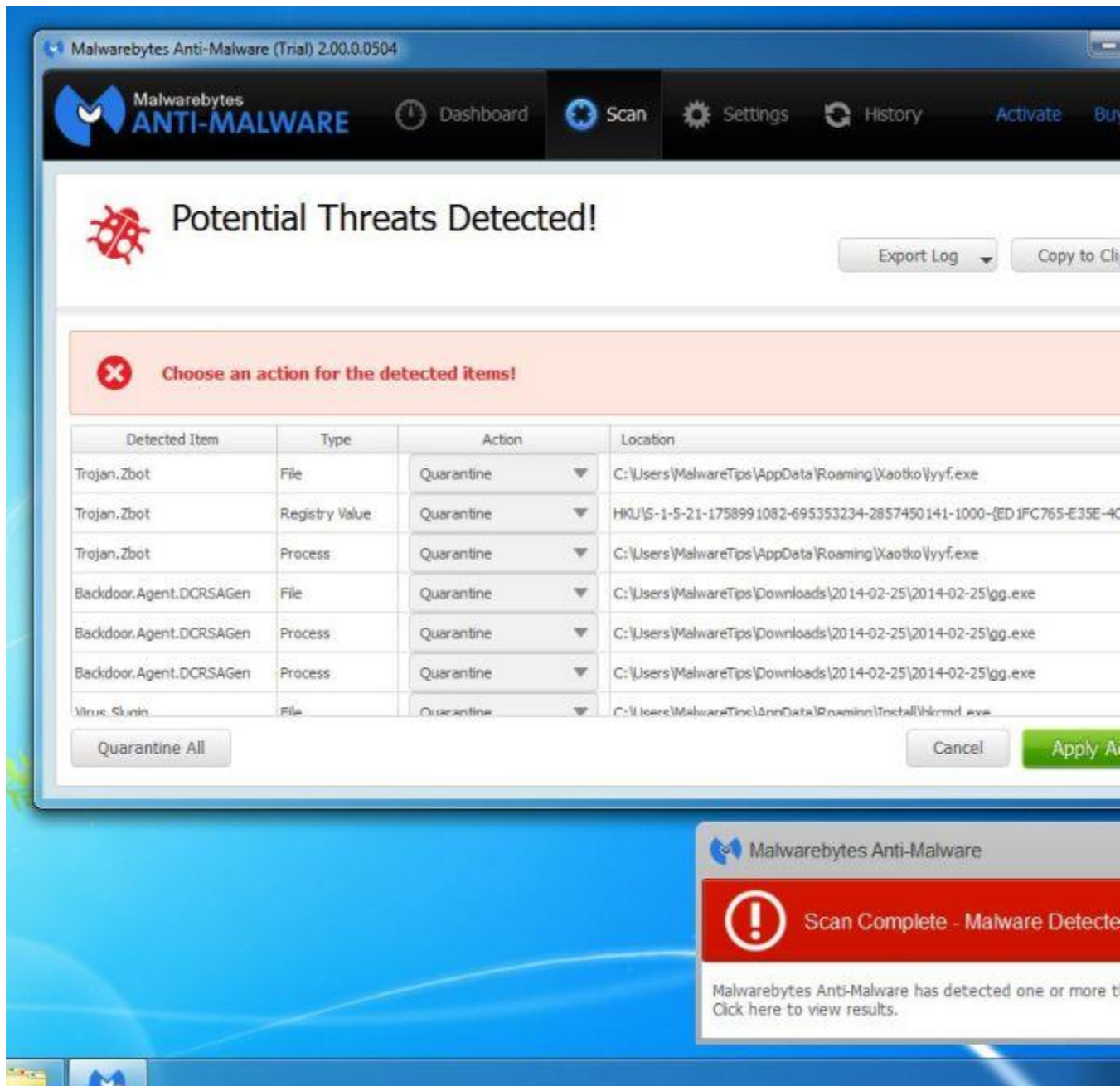
5. Malwarebytes Anti-Malware will now check for updates, and if there are any, you will need to click on the “**Update Now**” button.



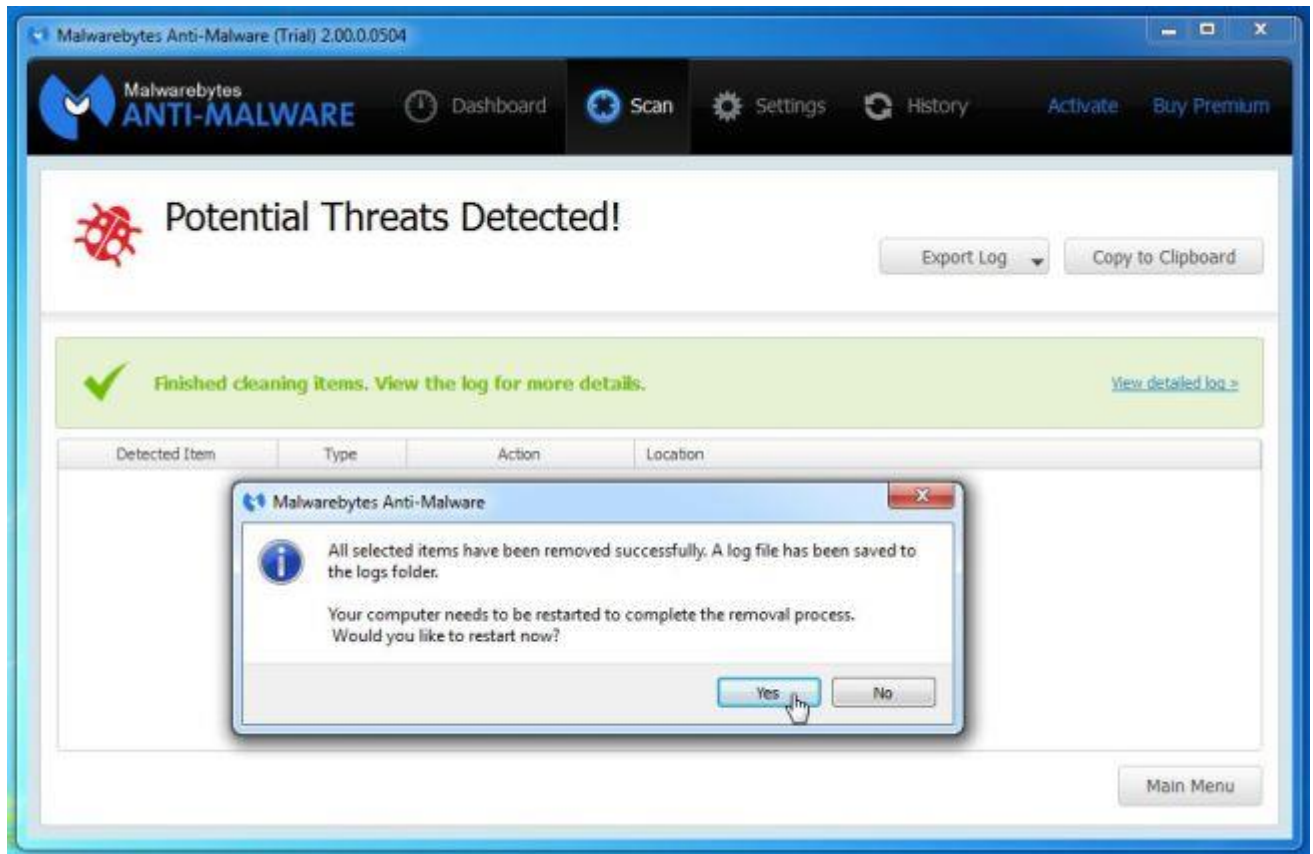
- Malwarebytes Anti-Malware will now start scanning your computer for the pop-up virus. When Malwarebytes Anti-Malware is scanning it will look like the image below.



- 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.



- 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

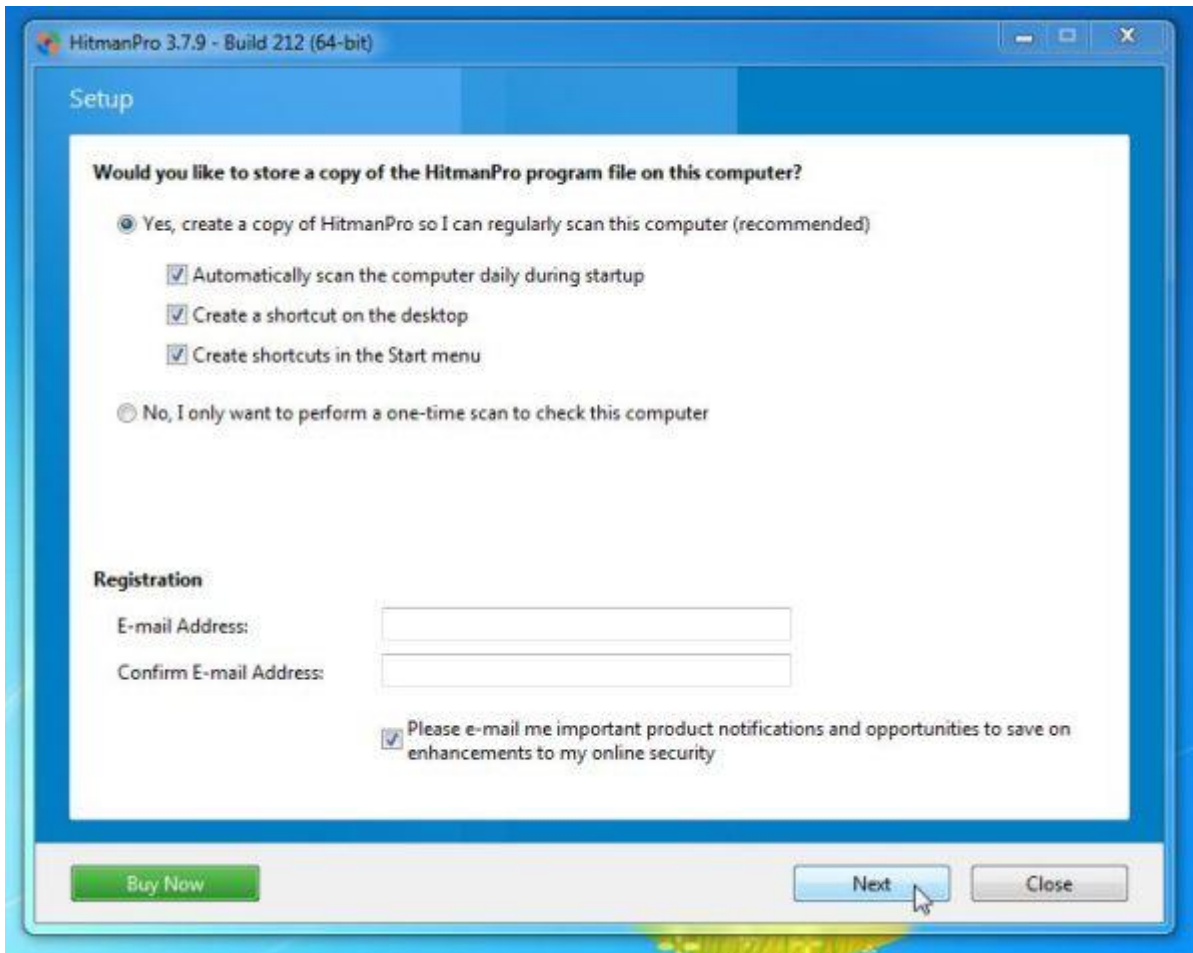
STEP 4: Remove stubborn rootkits from your computer with HitmanPro

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:
[HITMANPRO DOWNLOAD LINK](#) (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.



HitmanPro 3.7.9 - Build 212 (64-bit)

Setup

Would you like to store a copy of the HitmanPro program file on this computer?

Yes, create a copy of HitmanPro so I can regularly scan this computer (recommended)

Automatically scan the computer daily during startup

Create a shortcut on the desktop

Create shortcuts in the Start menu

No, I only want to perform a one-time scan to check this computer

Registration

E-mail Address:

Confirm E-mail Address:

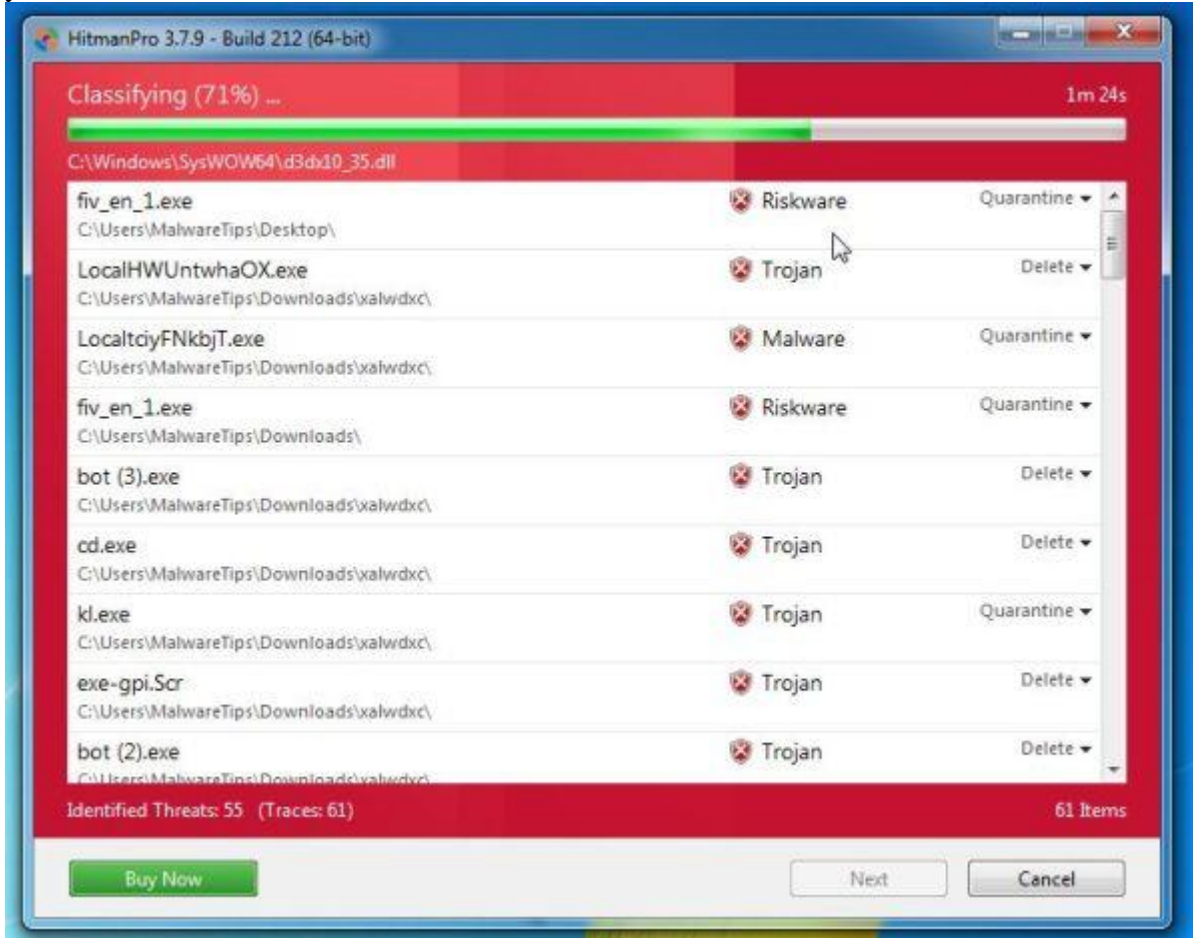
Please e-mail me important product notifications and opportunities to save on enhancements to my online security

Buy Now

Next

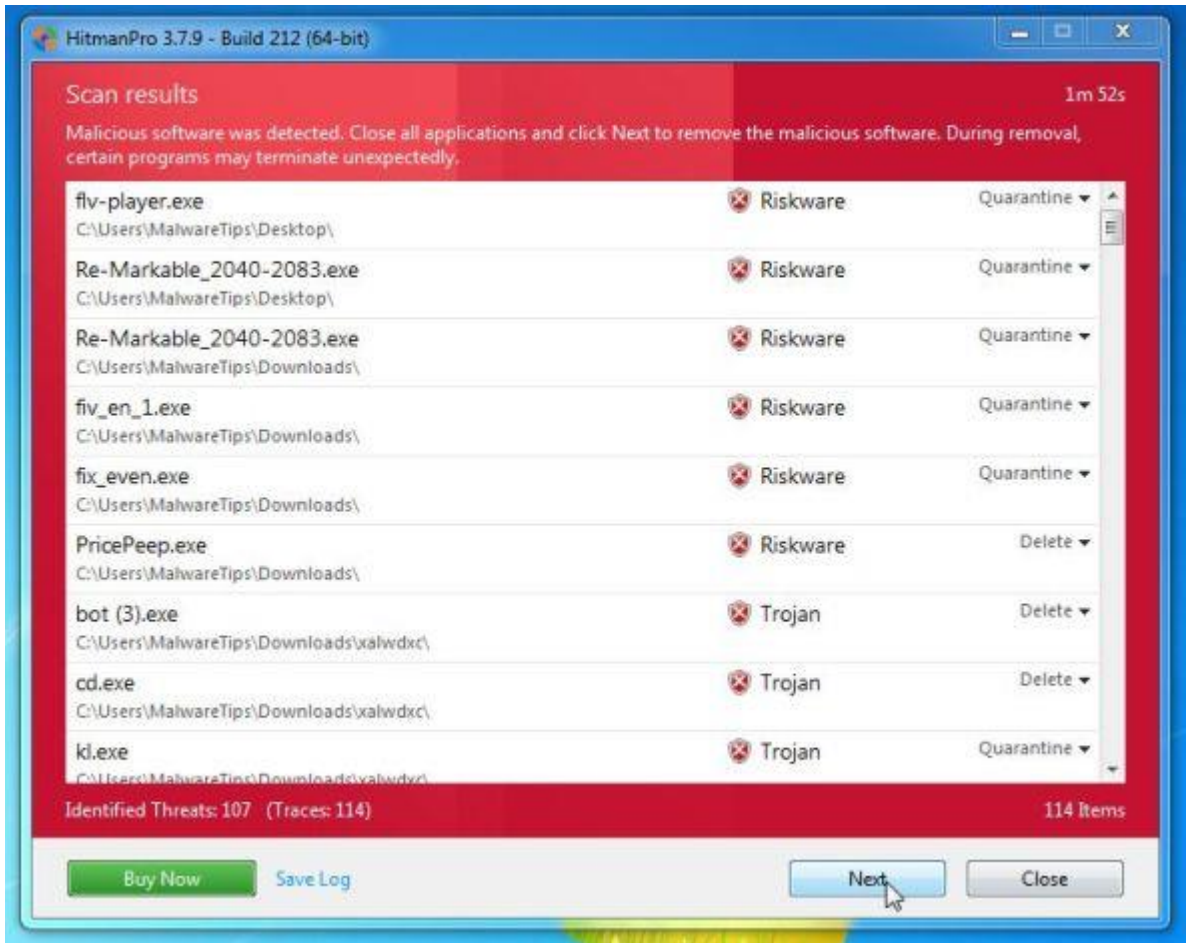
Close

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

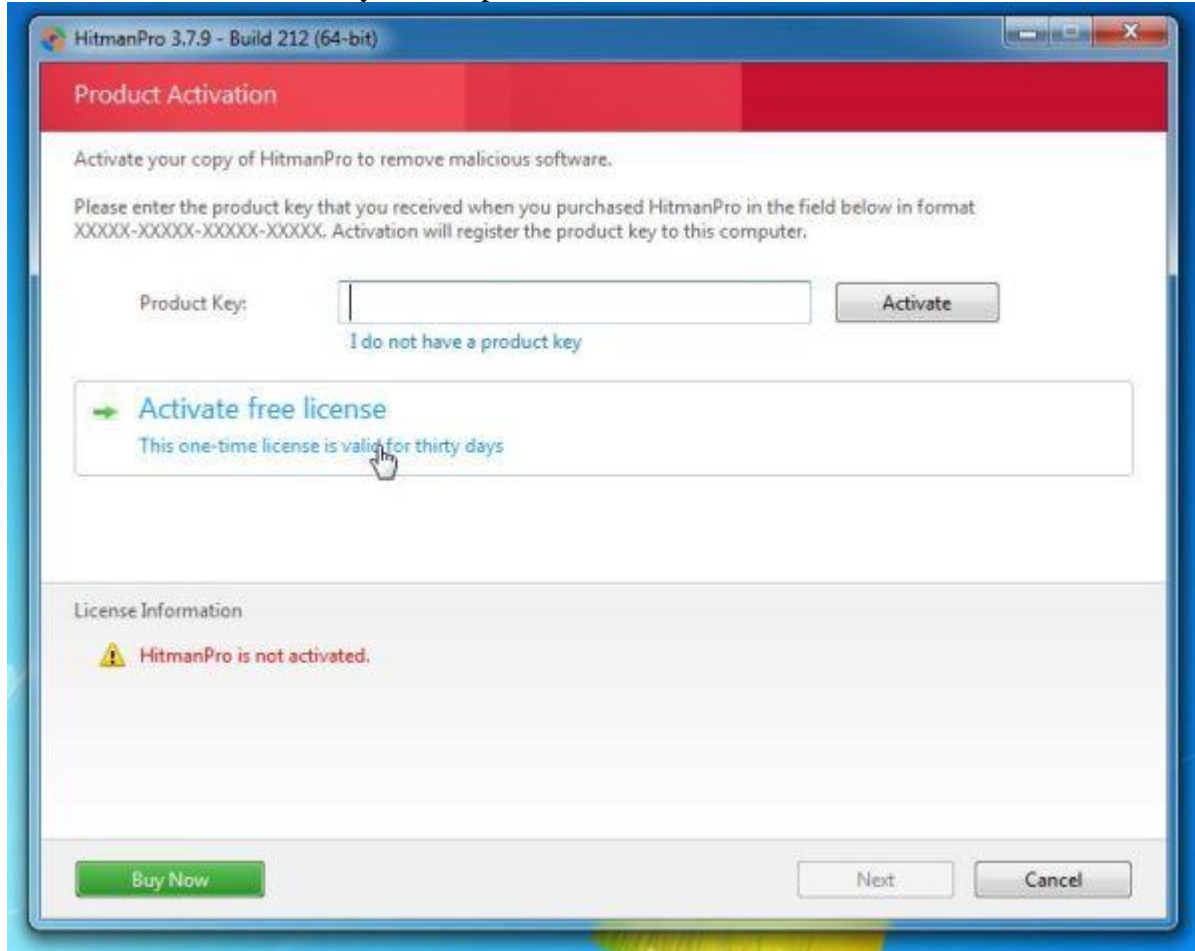


- When it has finished it will display a list of all the malware that the program found as shown in the image below. Click on the “Next” button, to remove any virus that has been

found.



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

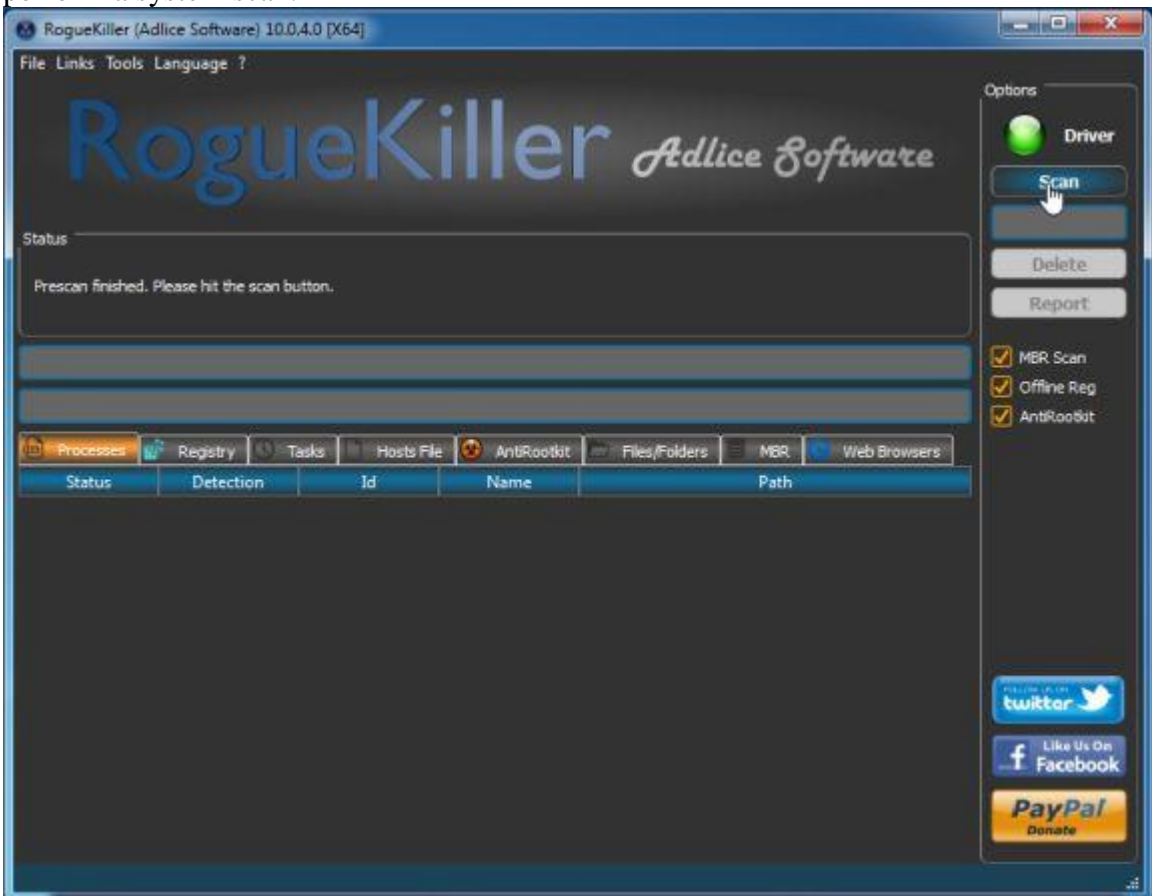


STEP 5: Remove the malicious registry keys added by malware with RogueKiller

RogueKiller is a utility that will scan for the unwanted registry keys and any other malicious files on your computer.

1. You can download the latest official version of **RogueKiller** from the below links.
 - [ROGUEKILLER x86 DOWNLOAD LINK](#) (For 32-bit machines)
 - [ROGUEKILLER x64 DOWNLOAD LINK](#) (For 64-bit machines)
2. Double-click on the file named “**RogueKiller.exe**” (for 32-bit versions of Windows) or “**RogueKillerX64.exe**” (for 64-bit versions of Windows). **Wait for the Prescan to complete.** This should take only a few seconds, then click on the “**Scan**” button to

perform a system scan.



3. After the scan has completed, click on the “Delete” button to remove Trojan.Poweliks!gm malicious registry keys or files.

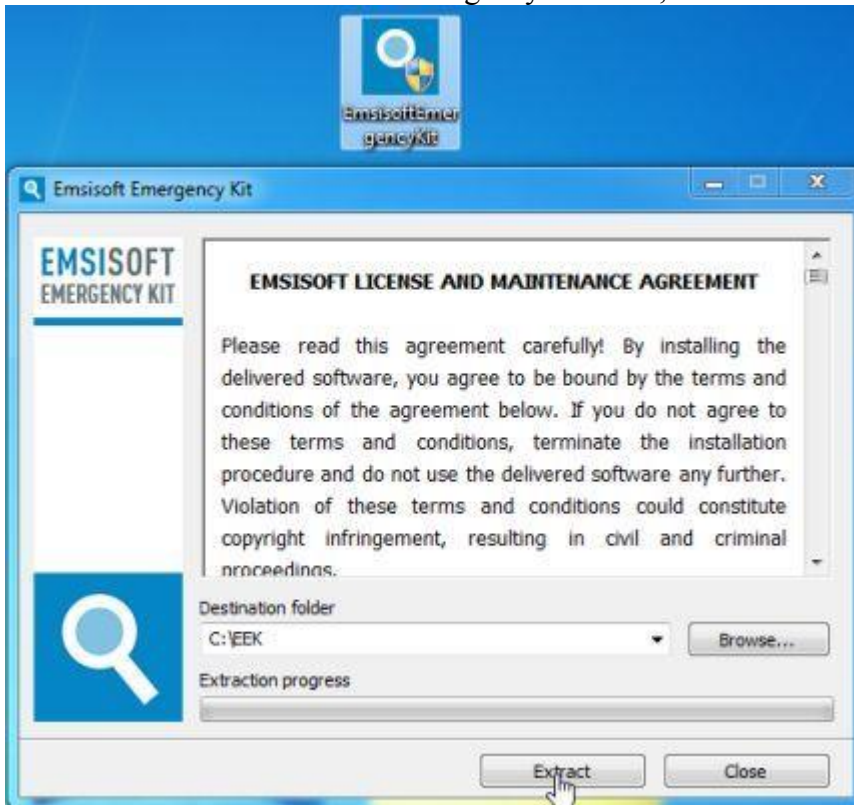


STEP 6: Double-check for any left over infections on your computer with Emsisoft Anti-Malware

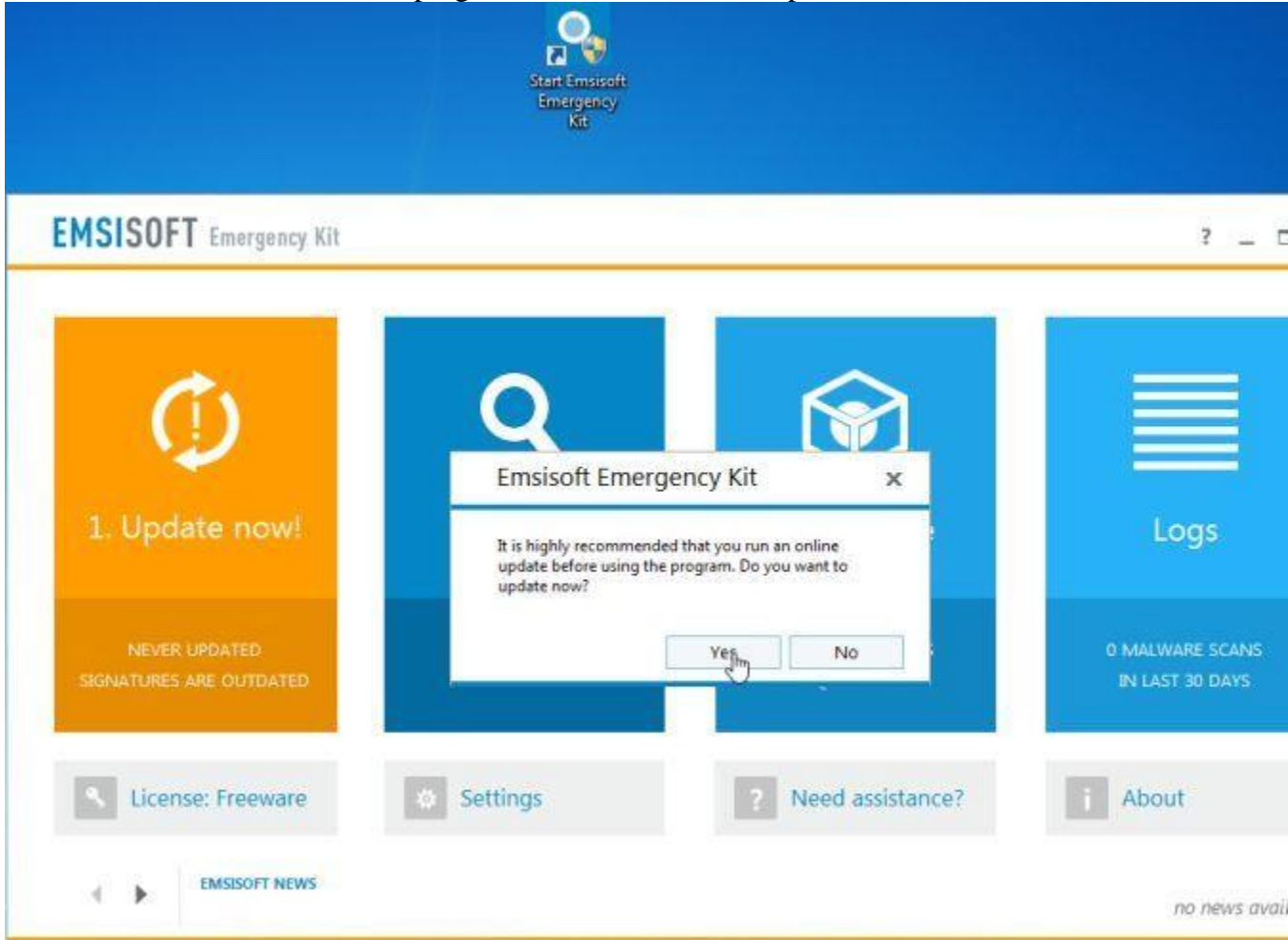
The Emsisoft Emergency Kit Scanner includes the powerful Emsisoft Scanner complete with graphical user interface. Scan the infected PC for Viruses, Trojans, Spyware, Adware, Worms, Dialers, Keyloggers and other malicious programs.

1. You can **download Emsisoft Emergency Kit** from the below link.
[EMSIISOFT EMERGENCY KIT DOWNLOAD LINK](#) ((This link will open a new web page from where you can download Emsisoft Emergency Kit)

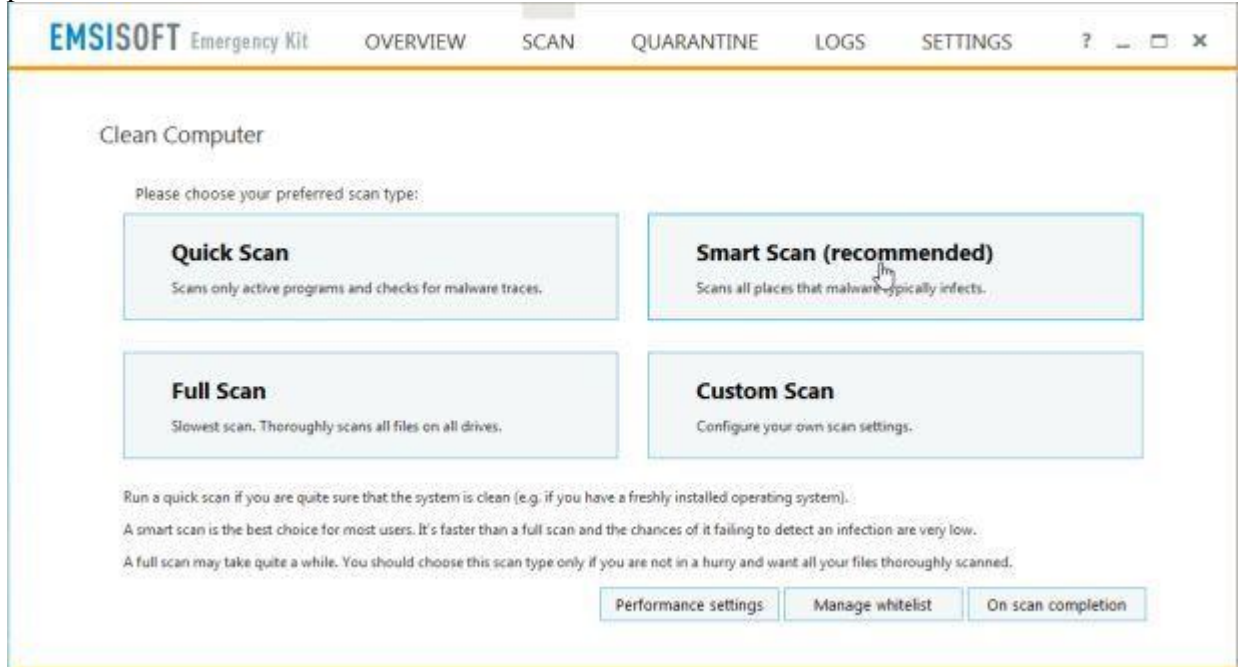
2. Double-click on the “EmsisoftEmergencyKit” icon, then click on the “**Extract**” button.



3. On your desktop you should now have a “**Start Extract Emsisoft Emergency Kit**” icon, double-click on it, then when the program will start allow it to update its database.



- Once the Emsisoft Emergency Kit has update has completed,click on the “Scan” tab, and perform a “Smart Scan”.



- When the scan will be completed,you will be presented with a screen reporting which malicious files has Emsisoft detected on your computer, and you'll need to click on **Quarantine selected objects** to remove them.

