COMODO
Creating Trust Online®

Comodo
Hijack Cleaner

Software Version 1.0

User Guide

Guide Version 1.0.120318

Comodo Security Solutions
1255 Broad Street
Clifton, NJ, 07013
United States

How to use Comodo Hijack Cleaner

Comodo Hijack Cleaner (CHC) is a lightweight scanner that identifies and removes all vulnerabilities from your internet browser. Such vulnerabilities include malicious add-ons, host file poisoning, fake search engines, unsafe home pages and untrusted DNS providers.

The application ensures:

- All browser extensions are safe
- Your browser uses a legitimate search engine
- Your home page and new blank page don't link to malware
- Your host file has not been contaminated
- Your desktop shortcuts open the correct browser and not a fake version
- Your browser uses a trusted DNS provider

CHC is a portable application which does not require installation. Just open the executable to start cleaning your computer.

Click the links below to jump to the respective explanation:

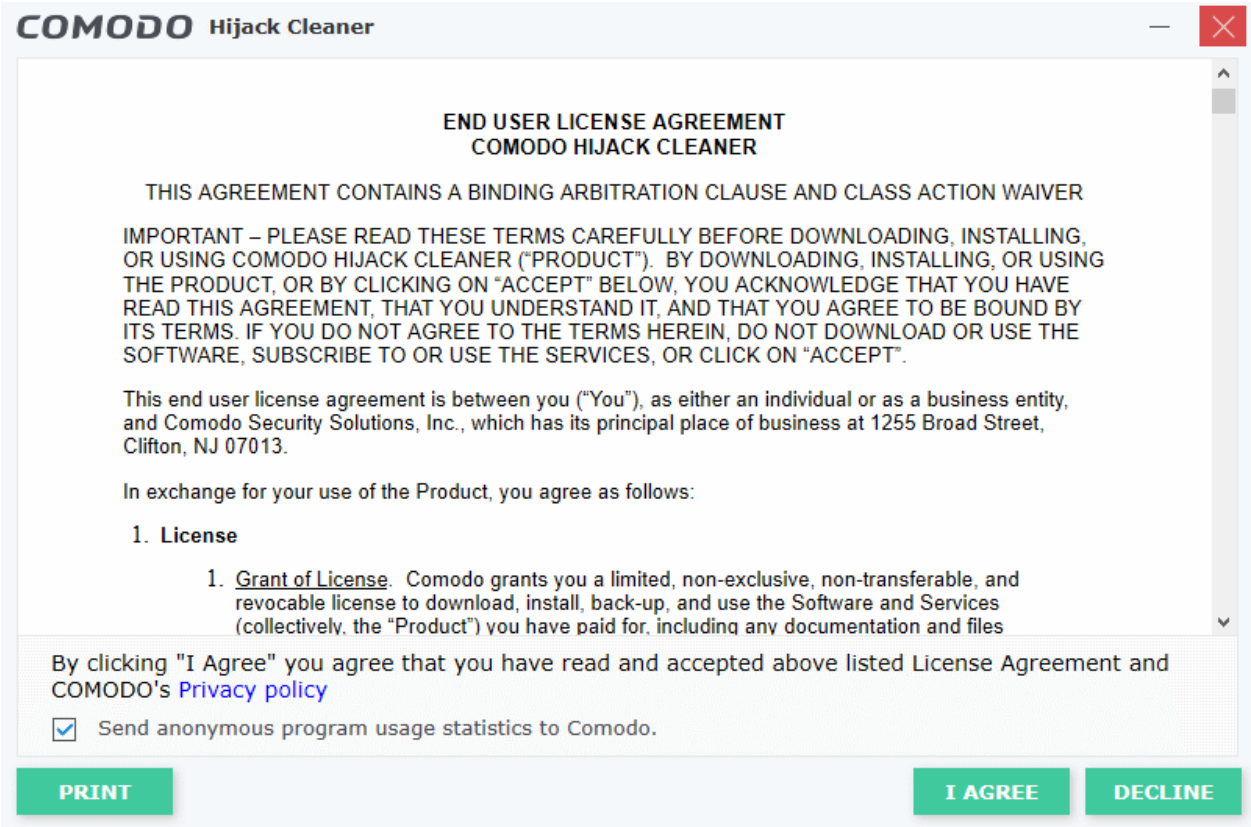
- **Download the application**
- **Run a scan**
- **Remove identified threats**
- **Configure Comodo Hijack Cleaner**

Download the application

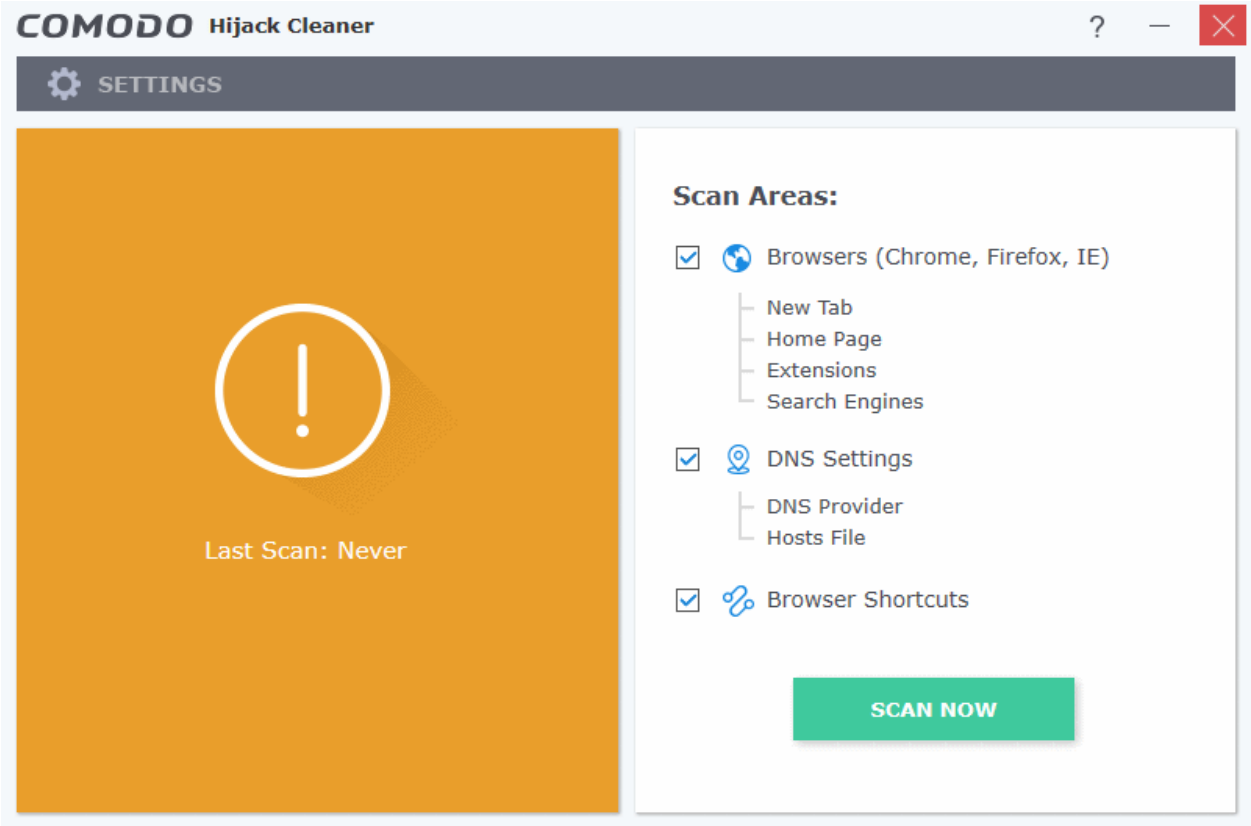
- Comodo Hijack Cleaner can be downloaded from https://download.comodo.com/chc/download/setups/chc.zip
- Extract the file and save it on your computer

Run a scan

- Open chc.exe
- Accept the end user license agreement:



- Send anonymous program usage statistics to Comodo - Comodo collects usage details so we can analyze how our users interact with CHC. This 'real-world' data allows us to create product improvements which reflect the needs of our users.
    - Enable this option to send your usage data to Comodo servers through a secure, encrypted channel.
    - Your privacy is not affected because the data is anonymized. Disable this option if you don't want to send usage details to Comodo.
- Read the license agreement and click 'I agree'.
- The main interface will open:



- Select the areas you want to scan:
  - **Browsers** - Scans the following items in Chrome, Firefox, Internet Explorer and Comodo Dragon/Ice Dragon:
    - Home page - Checks whether the page set as your homepage hosts or links to malware.
    - New Tab - Searches for malware hosted on the page you have set as your new tab page. CHC checks all linked pages if your new tab shows thumbnails of 'favorite' or 'recently visited' sites.
    - Extensions - Checks whether any enabled or disabled extension is malware, or links to malware.
    - Search Engines - Checks the legitimacy of the default search engine set for the browser. The default engine is used to search for the search terms you enter in the address bar. Your default search engine may be altered without your knowledge when you visit inappropriate websites. Illegitimate search engines can lead you to harmful websites that host malware or compromise your privacy.
  - **DNS Settings** - Checks that your Domain Name System (DNS) provider is a known-trusted provider, and that your host file does not redirect you to malicious websites.

Background Note:

- Domain name servers translate the domain names you see in your browser into machine-readable IP addresses. Think of a DNS server like a old-school telephone directory. The telephone directory 'pairs' a telephone number with a person's name. Similarly, a DNS server pairs a domain name with an IP address.
- For example, if you request a connection to www.comodo.com, your browser will first contact a DNS server to find out the IP address of www.comodo.com. The DNS server will reply to your browser with the correct IP address, in this case 91.199.212.176. Your browser will actually connect to 91.199.212.176, but will represent this connection as 'www.comodo.com' in your browser address bar.

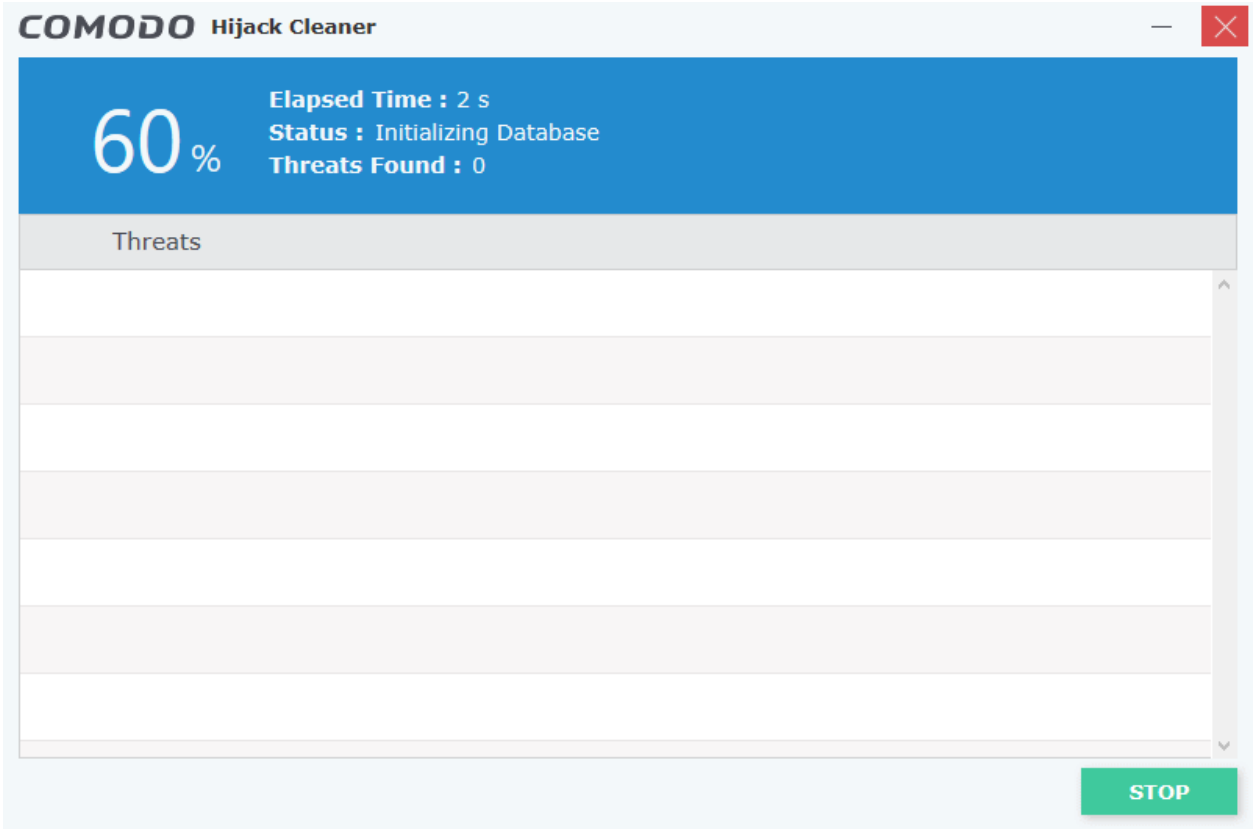
- If an attacker changes your DNS provider then they could send you to IP addresses that host malicious content, instead of the domain you requested.

CHC scans the following DNS and internet connection settings on your computer:

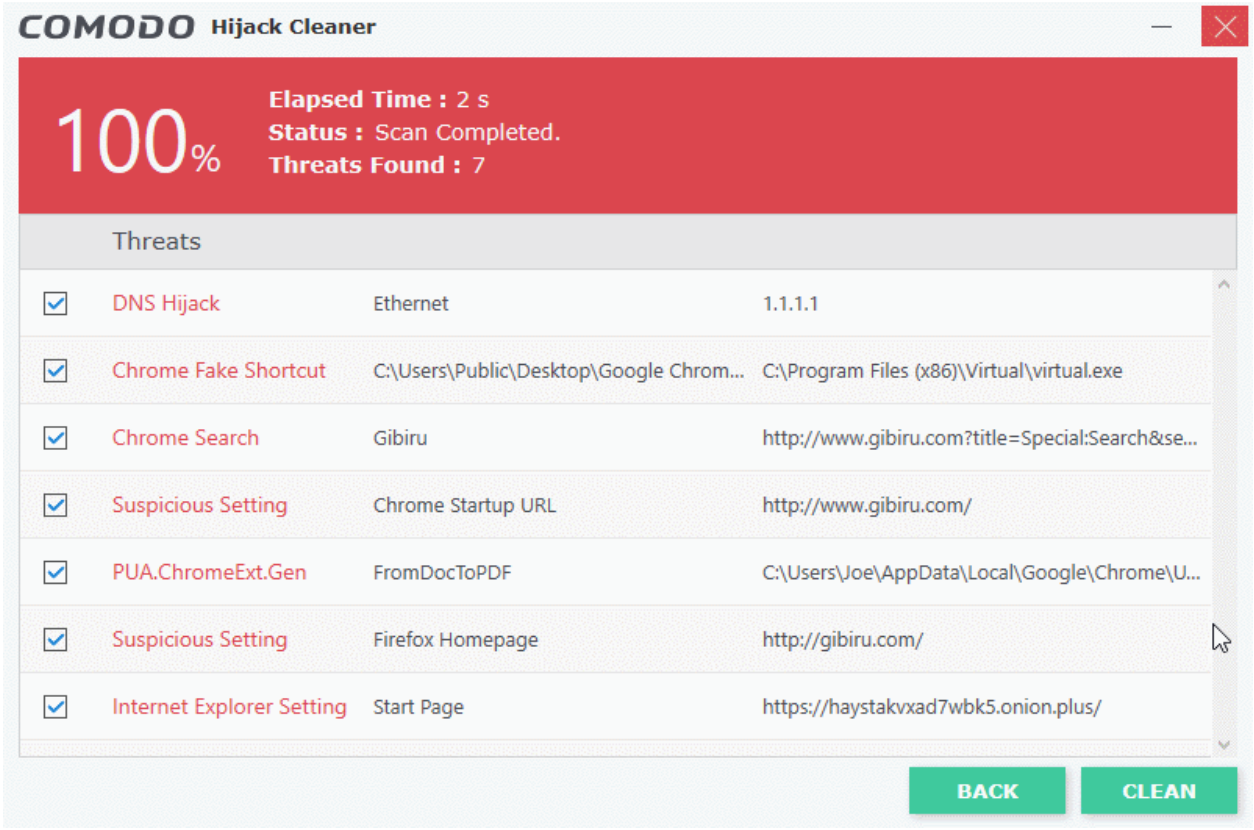
- **DNS Provider** - Checks that the DNS server used by your computer is on a list of bona-fide DNS providers. If your DNS server is not recognized, CHC will offer to change it to Google's public DNS servers. See **DNS Provider** under **Clean threats** for more details.
- **Hosts File** - CHC checks that your local host file has not been poisoned. Attackers can add entries to this file to send you to harmful websites.
  - Your host file contains a list of IP address and host name pairs. The file tells internet browsers that a specific domain name is located at a specific IP address.
  - The host file is often used by web-developers who wish to point a domain to an internal IP address for testing. Your browser will use the information in the host file instead of contacting a public DNS server as explained above.
  - For example, the web-dev might want to you to connect to an IP address of 192.168.0.0 if you type 'example.com' into your browser. In this example, '192.168.0.0' is the IP address of the internal server that hosts test content for example.com.
  - Your hosts file can be found at '*c:/windows/system32/drivers/etc/hosts*'. If you are a home user, there is little-to-no reason why your host file should contain any additional IP/domain pairs. Any IP/domain pairs you see below the '#' content are worth investigating.
- **Browser Shortcuts** - CHC scans the browser shortcuts on the desktop, start menu, quick launch bar have not been sabotaged so they open a different application or a hacked version of the browser.

- Click 'SCAN NOW'

The application will first download the updated domain whitelist/blacklist from Comodo servers and start scanning the selected locations.



On completion of scanning, the results will be displayed.



Remove identified threats

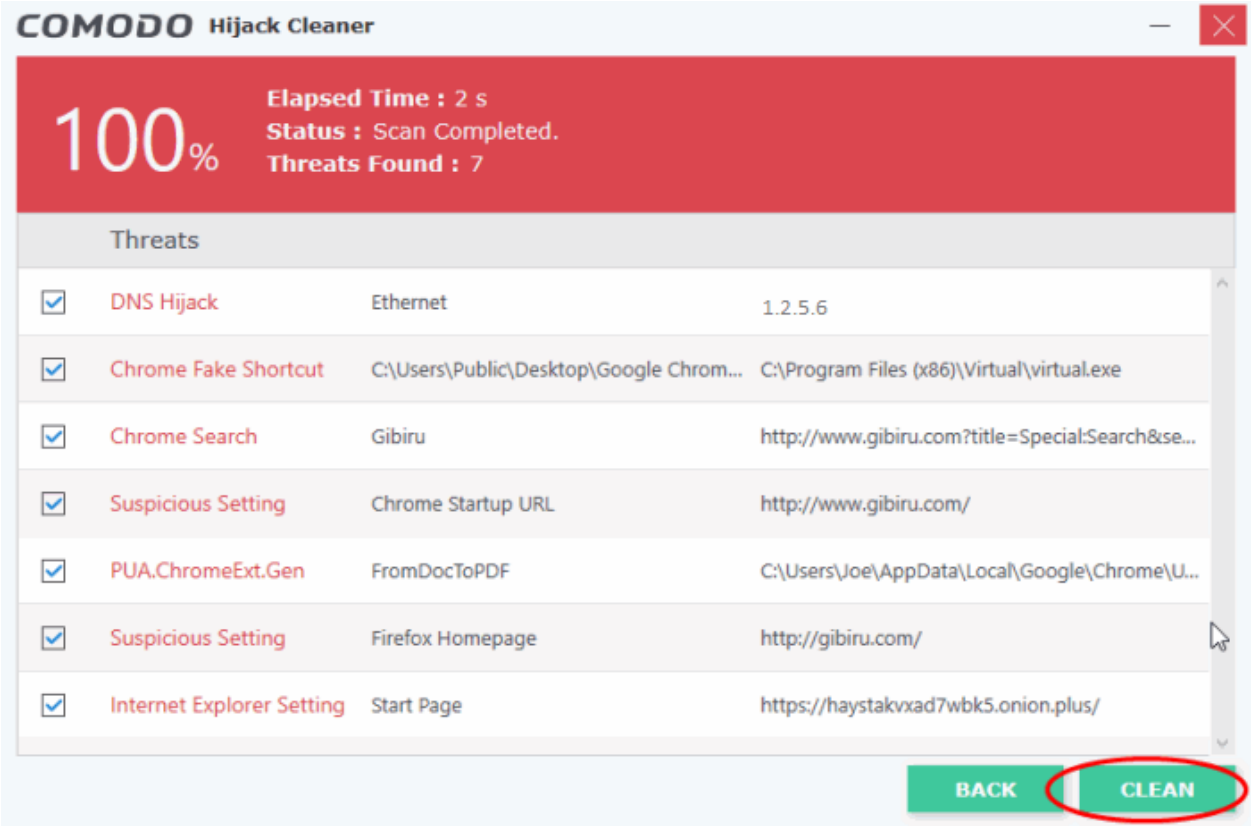
The results screen shows threats identified by the scan and allows you to:

- **Clean threats**

- **Add false positives to exclusion**
- **Submit a false positive to Comodo for inclusion in whitelist**

Clean threats

- Select the item(s) you want to remove and click the 'Clean' button



Items you clean are reconfigured as follows:

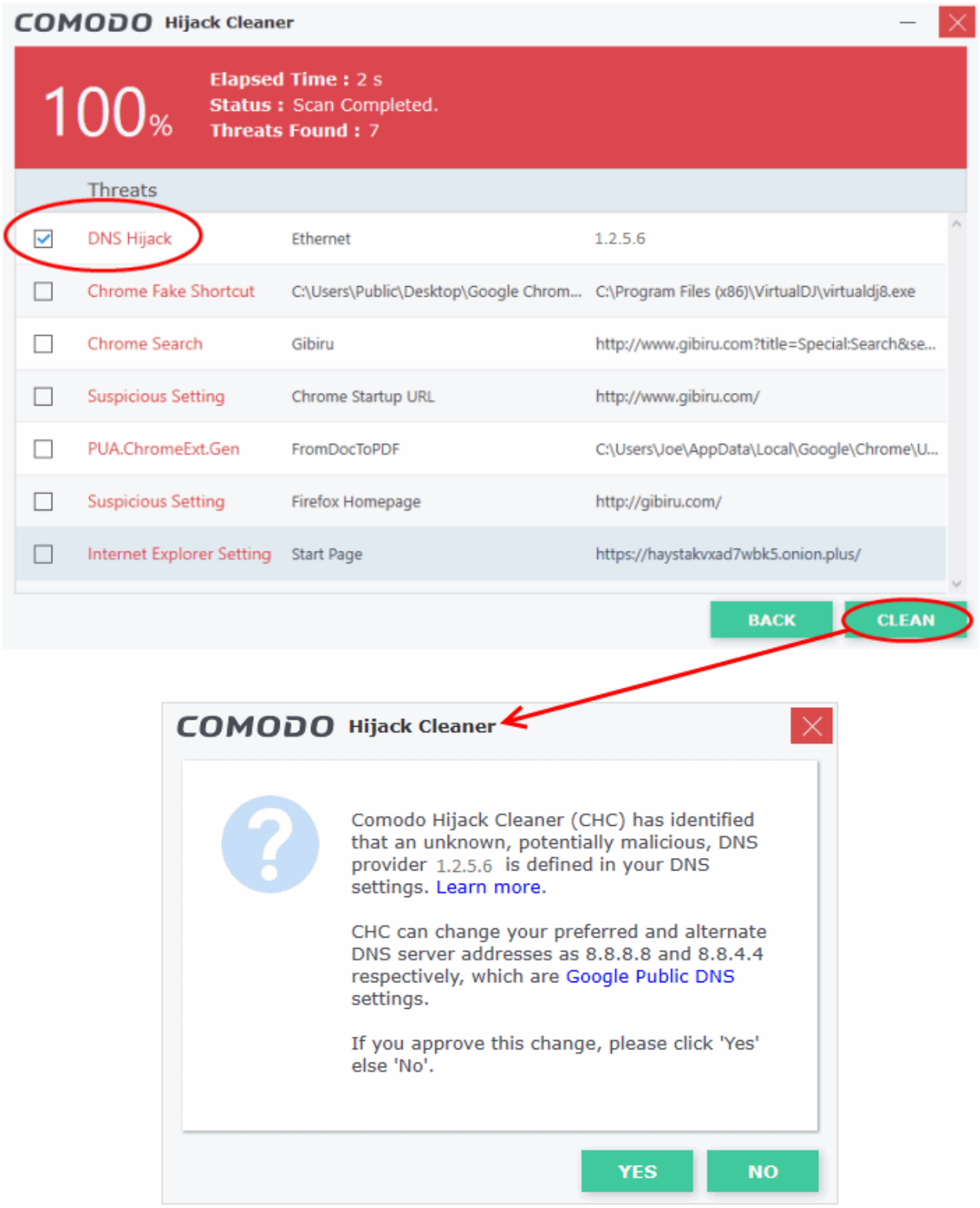
Browser Home Page - Your home page is set to Google - **https://www.google.com**

New tab - Malicious links and pages are removed

Extensions - The extension(s) is uninstalled

Search Engine - Your search engine is set to Google

DNS Provider - Your DNS provider will be set to Google DNS. You have to approve this change. A confirmation dialog is shown as follows:



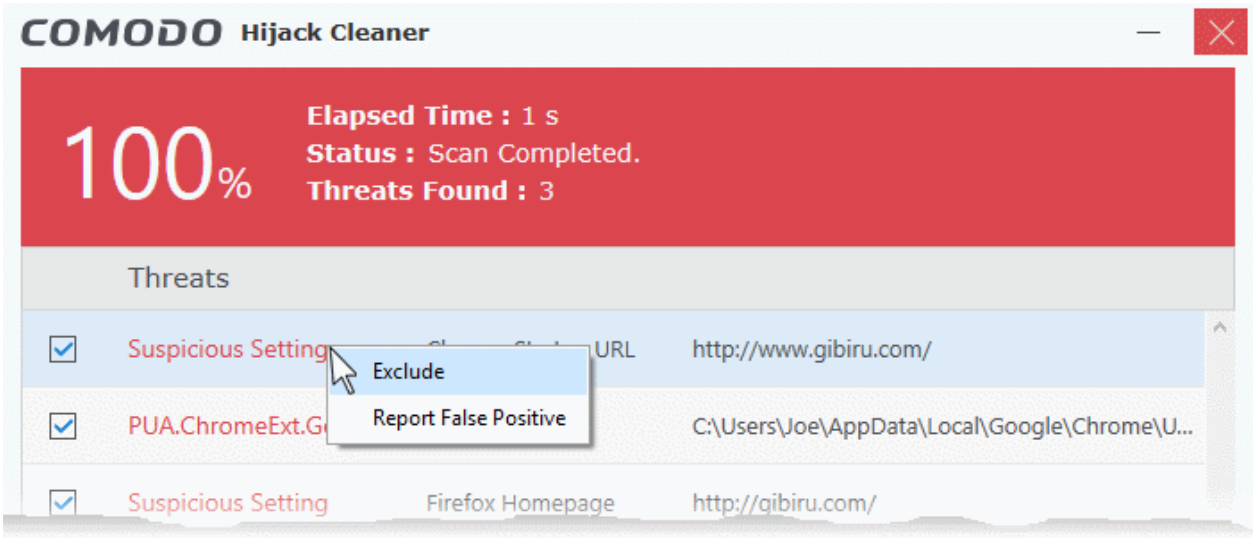
- Click 'Yes' in the confirmation dialog to change DNS settings to Google DNS
- Click 'No' if you want to manually reconfigure your DNS settings

Hosts File - Any malicious host file entries are removed.

Browser Shortcuts - Shortcut(s) will be reconfigured to point to the genuine browser

Add false positives to exclusion

- Add an item to exclusions if you do not want it to be flagged by future scans.
- Right-click on the item from the results screen and choose 'Exclude'

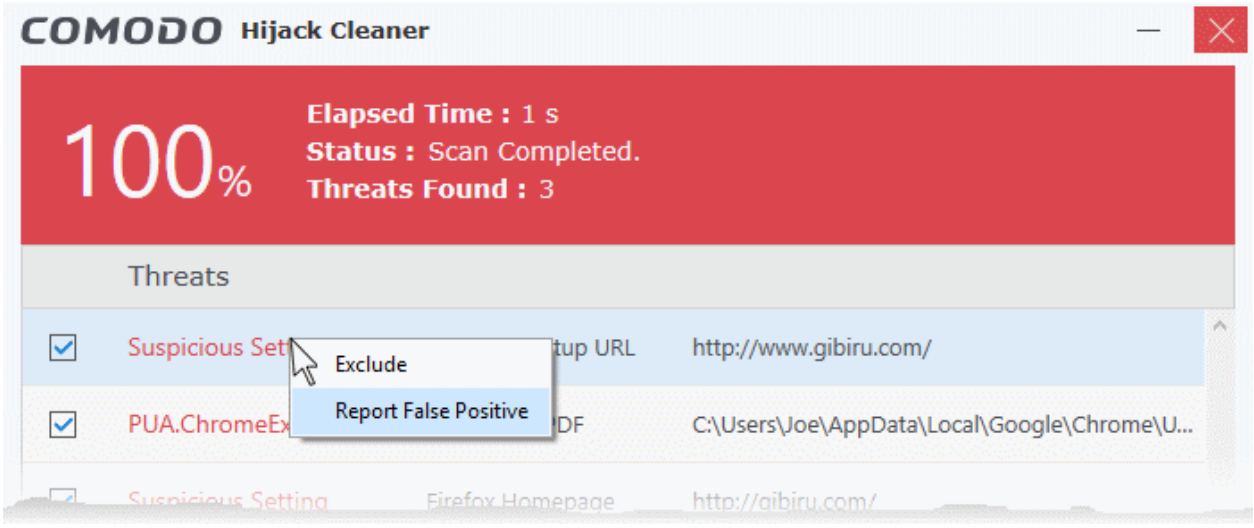


The item will be added to exclusions and skipped in the future scans. You can manage exclusions from the 'Settings' screen. See '**Configure Comodo Hijack Cleaner**' for ore details.

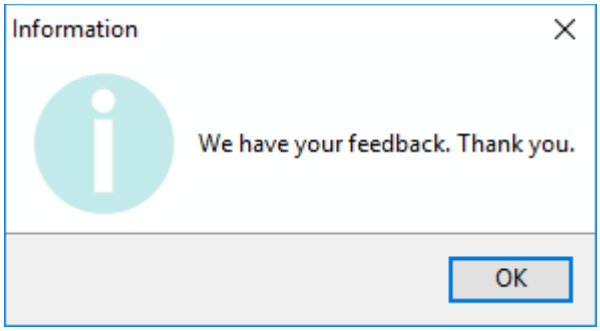
Submit a false positive to Comodo for inclusion in whitelist

If you are sure that an item identified as a threat is actually safe, then you can submit it to Comodo for testing. If confirmed as a false-positive, the item will be added to the global white-list.

- Right-click on the item from the results screen and choose 'Report as False Positive'



The file will be uploaded to Comodo Servers.

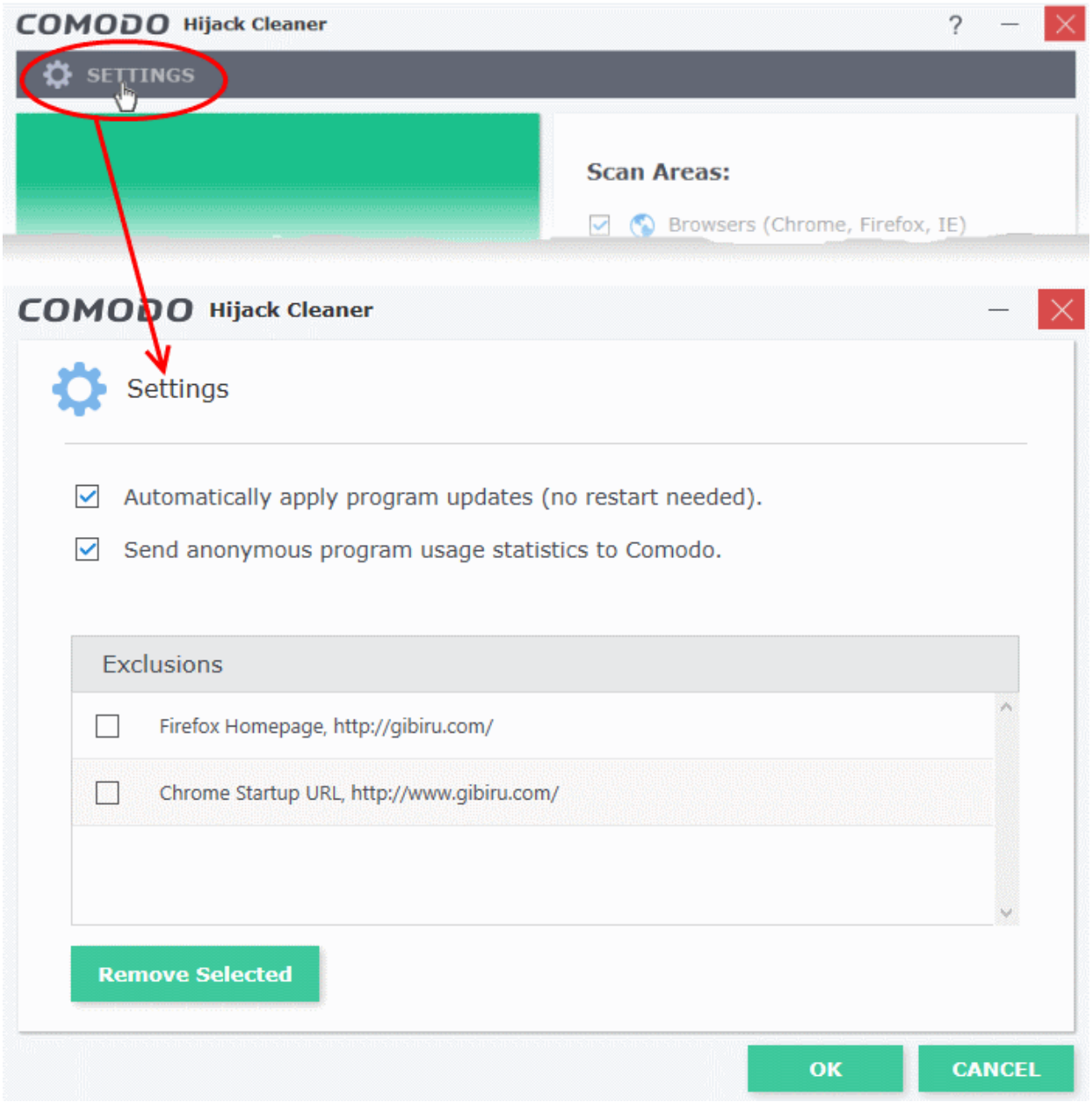


Configure Comodo Hijack Cleaner

The 'Settings' screen allows you to configure update settings of the application and to manage the items added to the exclusions.

To configure CHC and manage exclusions

- Click 'Settings' on the top left of the interface



- Automatically apply program updates - CHC will check for and install available updates every time you start the application.
    - If you deselect this option then you will instead see an alert when a new version is available.
- Send anonymous program usage statistics to Comodo - Comodo collects usage details so we can analyze how our users interact with CHC. This real-world data allows us to create product improvements which reflect the needs of our users. Your privacy is not affected because the data is anonymized.
- Exclusions - A list of items you have told CHC to ignore during a scan.
    - Select an item and click 'Remove Selected' if you no longer want it to be skipped.
    - The item will be identified as a threat during the next scan, unless it has been white-listed since the time you added it to exclusions.
- Click 'OK' for your settings to take effect.

About Comodo Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets.

About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit comodo.com or our **blog**. You can also follow us on **Twitter** (@ComodoDesktop) or **LinkedIn**.

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.888.266.636

Tel : +1.703.581.6361

https://www.comodo.com

Email**: EnterpriseSolutions@Comodo.com**