HulaToo là gì? Làm sao để gỡ bỏ HulaToo?

Phần mềm quảng cáo HulaToo được thiết kế để chỉnh sửa các thiết lập trình duyệt và có thể cài đặt thêm các plugin (toolbars, extensions (tiện ích mở rộng) hoặc add-ons) trên trình duyệt web để "*chèn thêm*" các link quảng cáo vào đó. Ngoài ra chương trình này còn có thể điều hướng máy tính người dùng đến các trang web độc hại hoặc có thể cài đặt thêm các chương trình độc hại để "thỏa hiệp" vấn đề bảo mật trên máy tính người dùng.

Phần 1: HulaToo là gì?

"*HulaToo*" là một **phần mềm quảng cáo độc hại,** nếu HulaToo được cài đặt trên máy tính, nó sẽ chỉnh sửa các thiết lập hệ thống để hiển thị các cửa sổ popup quảng cáo kiếm tiền hoặc điều hướng các trình duyệt web đến các trang web chứa quảng cáo. Và nếu máy tính của bạn bị HulaToo tấn công, trên màn hình máy tính sẽ hiển thị các cửa sổ quảng cáo. Và đây cũng là một trong những **nguyên nhân khiến máy tính của bạn ngày một chậm dần bởi các chương trình độc hại chạy trên nền background**.

Phần mềm quảng cáo HulaToo được thiết kế để chỉnh sửa các thiết lập trình duyệt và có thể cài đặt thêm các plugin (toolbars, extensions (tiện ích mở rộng) hoặc add-ons) trên trình duyệt web để "chèn thêm" các link quảng cáo vào đó. Ngoài ra chương trình này còn có thể điều hướng máy tính người dùng đến các trang web độc hại hoặc có thể cài đặt thêm các chương trình độc hại để "thỏa hiệp" vấn đề bảo mật trên máy tính người dùng.

Về mặt kỹ thuật, HulaToo không phải là một dạng virus mà nó được phân loại là một chương trình không mong muốn (PUP - Potentially Unwanted Program) có thể chứa và cài đặt các chương trình độc hại trên máy tính của bạn, chẳng hạn như adware (các phần mềm quảng cáo), toolbars hoặc virus. Nếu máy tính của bạn bị "nhiễm" các phần mềm quảng cáo, khi đó trên màn hình máy tính của bạn sẽ liên tục xuất hiện các cửa sổ popup quảng cáo, banner và các liên kết tài trợ hoặc trong một số trường hợp tốc độ duyệt Web của các trình duyệt bị chậm do các chương trình độc hại chạy trên nền background.

Chương trình quảng cáo HulaToo được cài đặt trên hệ thống mà người dùng không hề hay biết, lí do là bởi vì các chương trình này được đóng gói bên trong các phần mềm miễn phí khác và khi người dùng tải các phần mềm này về cài đặt thì vô tình cài đặt cả các chương trình quảng cáo cáo HulaToo.

Vì lý do này mà khi cài đặt bất cứ một chương trình nào trên máy tính bạn nên:

- Trên màn hình cài đặt ứng dụng, không nên click chọn nút Next quá nhanh.
- Đọc kỹ các điều khoản trước khi click chọn Accept (chấp nhận).
- Luôn luôn chọn "Custom" installation – tùy chỉnh cài đặt.
- Từ chối việc cài đặt các phần mềm bổ sung mà bạn không muốn cài đặt.

- Bỏ tích bất kỳ các tùy chọn nói rằng trang chủ và các cài đặt tìm kiếm sẽ bị chỉnh sửa.

Phần 2: Gỡ bỏ tận gốc HulaToo

Bước 1: Gỡ bỏ cài đặt HulaToo trên máy tính Windows

Bước đầu tiên bạn cần làm là tìm và gỡ bỏ chương trình HulaToo được cài đặt trên máy tính của mình.

1. Truy cập menu Uninstall.

- Trên Windows 7 và Windows Vista:

Nếu sử dụng Windows XP, Windows Vista và Windows 7, click chọn nút **Start**, sau đó click chọn **Control Panel**.

- Trên Windows 10 và Windows 8:

Để gỡ bỏ cài đặt một chương trình trên máy tính Windows 10 hoặc Windows 8, đầu tiên bạn kích chuột phải vào nút Start rồi chọn **Control Panel**.

2. Trên cửa sổ Control Panel, click chọn tùy chọn "*Uninstall a program*" nằm tại mục **Programs**.

Nếu đang sử dụng Classic View trên Control Panel, bạn kích đúp chuột vào biểu tượng Programs and Features.

3. Trên cửa sổ Programs and Features hoặc Uninstall a Program, cuộn xuống danh sách các chương trình được cài đặt gần đây, sau đó tìm và gỡ bỏ cài đặt chương trình HulaToo.

- Ngoài ra tìm và gỡ bỏ cài đặt các chương trình không rõ nguồn gốc.

- Để xem các chương trình mới được cài đặt gần đây, bạn click chọn Installed On để sắp xếp các ứng dụng theo ngày. Sau đó cuộn xuống danh sách và gỡ bỏ cài đặt các chương trình không mong muốn đi.

- Nếu gặp sự cố trong quá trình gỡ bỏ cài đặt các chương trình độc hại trên, bạn có thể sử dụng Revo Uninstaller để gỡ bỏ hoàn toàn các chương trình không mong muốn trên máy tính của mình.

Bước 2: Gỡ bỏ phần mềm quảng cáo HulaToo trên trình duyệt Internet Explorer, Firefox và Chrome bằng AdwCleaner

AdwCleaner là một tiện ích miễn phí, tiện ích này sẽ quét hệ thống và các trình duyệt web để tìm và loại bỏ các chương trình quảng cáo, các tập tin độc hại HulaToo, và các tiện ích mở rộng không mong muốn được cài đặt trên trình duyệt mà bạn không hề hay biết.

1. Tải AdwCleaner về máy và cài đặt.

2. Trước khi cài đặt AdwCleaner, đóng tất cả trình duyệt web trên máy tính của bạn, sau đó kích đúp chuột vào biểu tượng AdwCleaner.

Nếu Windows hỏi bạn có muốn cài đặt AdwCleaner hay không, click chọn **Yes** để cho phép chạy chương trình.

3. Khi chương trình đã mở, click chọn nút **Scan** như hình dưới đây:

Và AdwCleaner sẽ bắt đầu quá trình quét để tìm và loại bỏ các chương trình quảng cáo (adware) cũng như các chương trình độc hại khác.

4. Để loại bỏ các tập tin độc hại **Babylon Toolbar được AdwCleaner** phát hiện, click chọn nút **Clean**.

5. AdwCleaner sẽ thông báo bạn lưu lại bất kỳ các tập tin hoặc tài liệu nào mà bạn đang mở vì chương trình cần phải khởi động lại máy tính để hoàn tất quá trình dọn sạch các tập tin độc hại. Nhiệm vụ của bạn là lưu các tập tin và tài liệu lại, sau đó click chọn **OK**.

Bước 3: Dọn sạch virus HulaToo bằng Malwarebytes Anti-Malware Free

Malwarebytes Anti-Malware Free là công cụ quét hệ thống theo yêu cầu, công cụ sẽ tìm và loại bỏ tất cả các mối "đe dọa", các phần mềm độc hại (malware) khỏi máy tính của bạn, trong đó bao gồm worm, trojian, rootkit, rouge, dialer, spyware (phần mềm gián điệp),....

Và điều quan trọng hơn cả là Malwarebytes Anti-Malware sẽ chạy song song với các phần mềm diệt virus khác mà không xảy ra lỗi xung đột.

1. Tải Malwarebytes Anti-Malware về máy và cài đặt.

2. Sau khi đã tải xong Malwarebytes Anti-Malware Free, tiến hành đóng tất cả các chương trình lại, sau đó kích đúp chuột vào biểu tượng có tên **mbam-setup** để bắt đầu quá trình cài đặt Malwarebytes Anti-Malware Free.

Lúc này trên màn hình xuất hiện hộp thoại User Account Control hỏi bạn có muốn chạy tập tin hay không. Click chọn **Yes** để tiếp tục quá trình cài đặt.

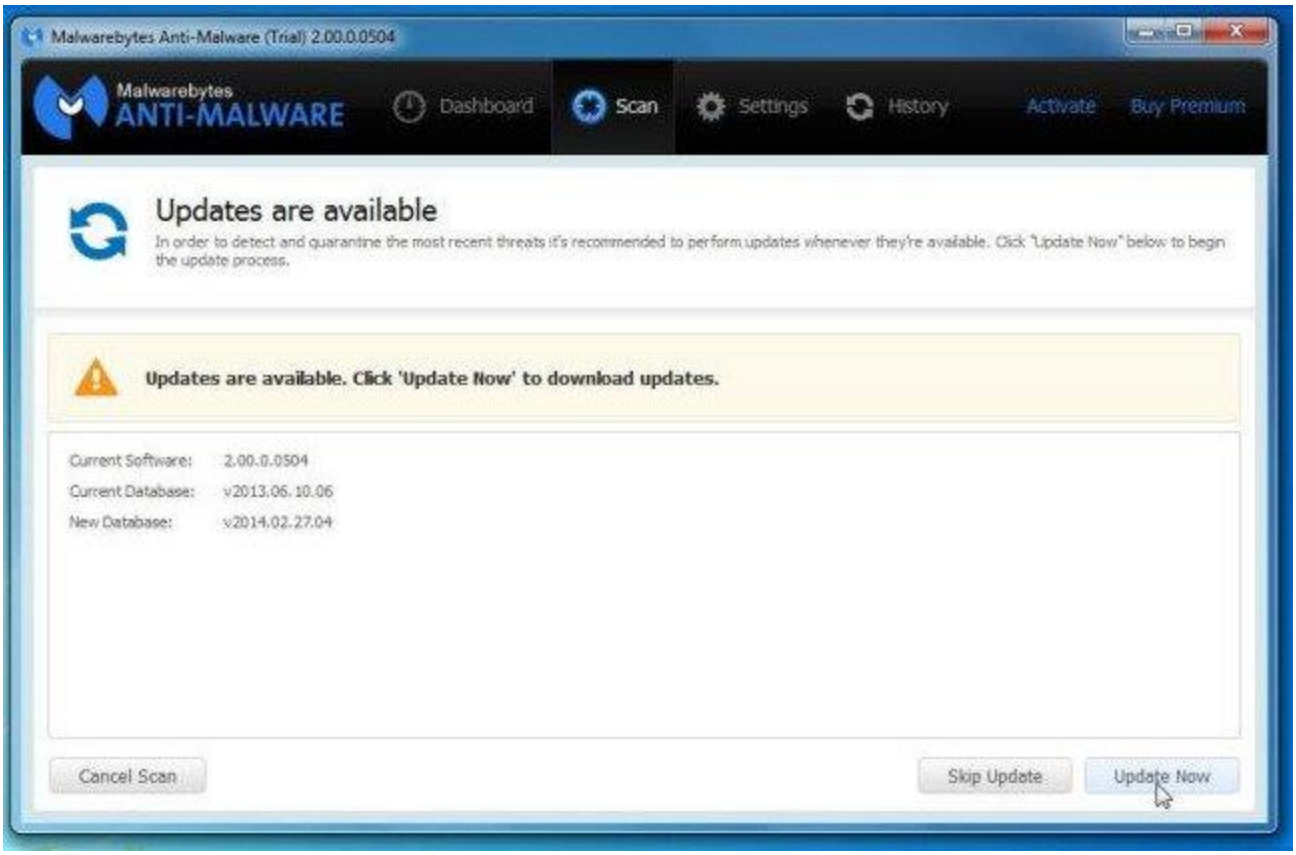
3. Thực hiện theo các bước hướng dẫn trên màn hình để cài đặt Malwarebytes Anti-Malware Setup Wizard.

Click chọn **Next** để thực hiện cài đặt Malwarebytes Anti-Malware, cho đến cửa sổ cuối cùng bạn click chọn **Finish** để hoàn tất.

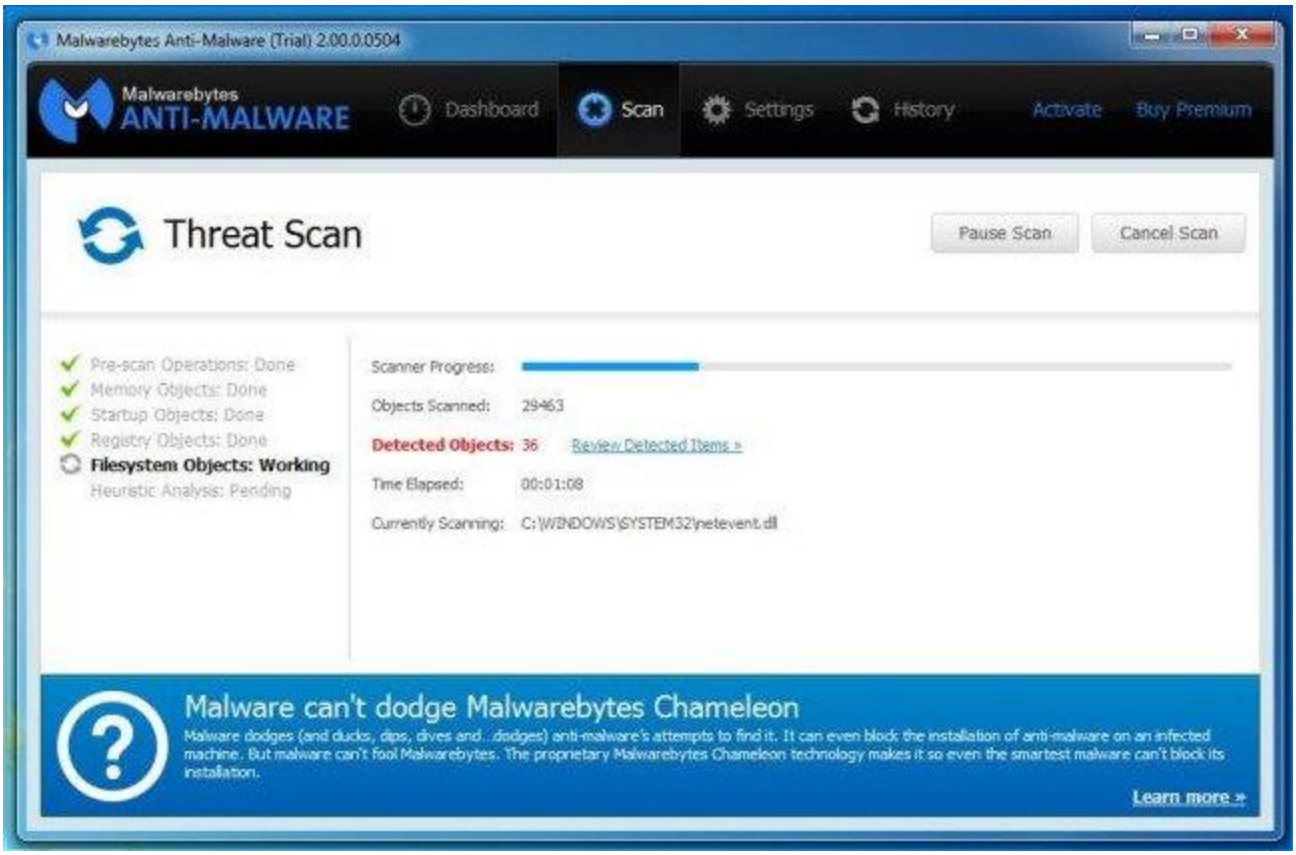
4. Sau khi cài đặt xong, Malwarebytes Anti-Malware sẽ tự động mở và update dữ liệu diệt virus. Để bắt đầu quá trình quét trên hệ thống bạn click chọn nút **Fix Now**.

Hoặc cách khác là bạn có thể click chọn **tab Scan** rồi chọn Threat Scan, sau đó click chọn **Scan Now**.

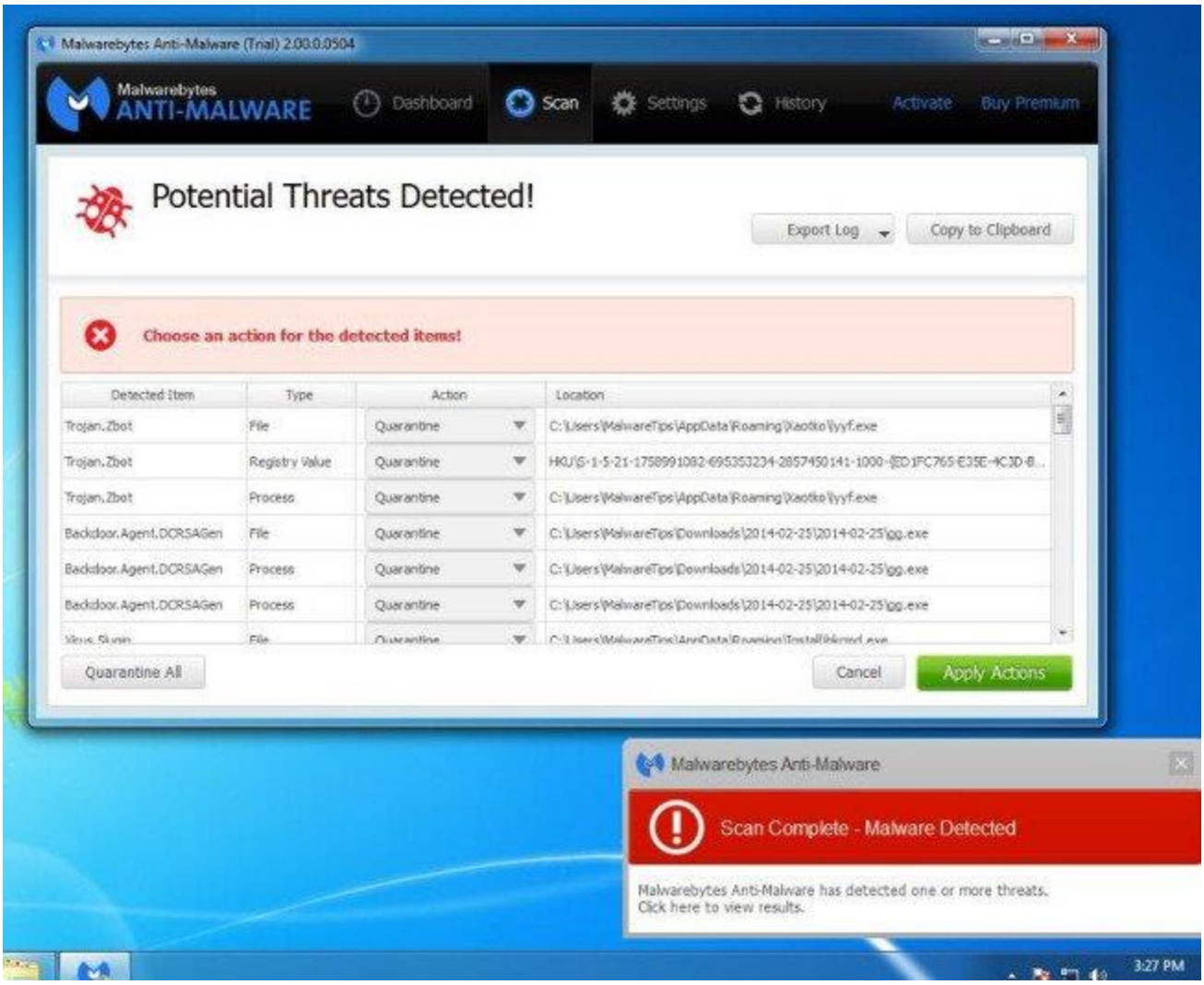
5. Malwarebytes Anti-Malware sẽ bắt đầu kiểm tra các bản cập nhật (update) mới nhất. Nếu có bất kỳ bản cập nhật mới nào, bạn click chọn nút **Update Now**.



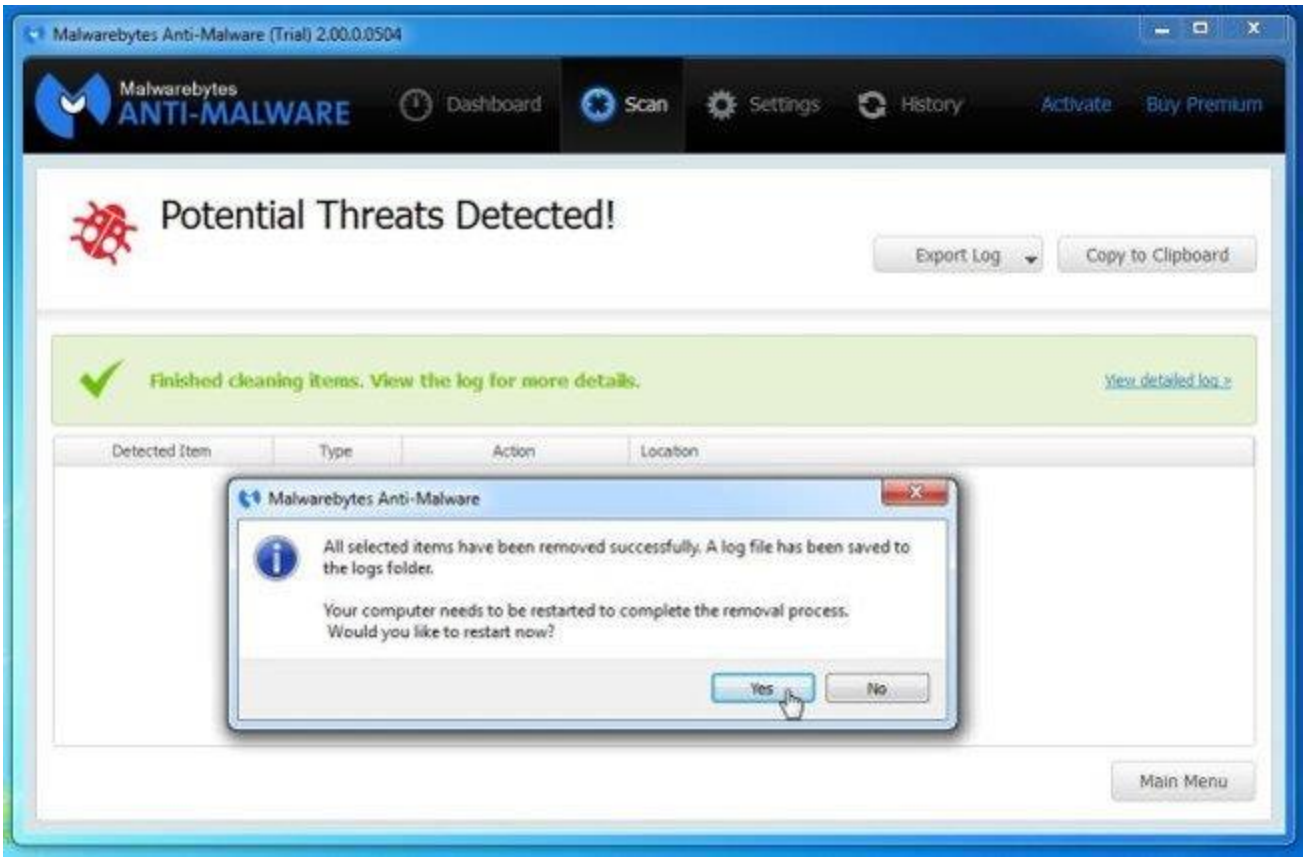
6. Malwarebytes Anti-Malware sẽ bắt đầu quét hệ thống của bạn để tìm và gỡ bỏ các chương trình, phần mềm độc hại trên hệ thống của bạn.



7. Sau khi kết thúc quá trình quét, trên màn hình sẽ xuất hiện cửa sổ hiển thị tất cả các tập tin, chương trình độc hại mà Malwarebytes Anti-Malware phát hiện được. Để gỡ bỏ các chương trình độc hại mà Malwarebytes Anti-Malware phát hiện được, click chọn nút Quarantine All, sau đó click chọn nút **Apply Now**.



8. Malwarebytes Anti-Malware sẽ loại bỏ tất cả các tập tin, chương trình độc hại và key registry mà nó phát hiện. Trong quá trình loại bỏ các tập tin này, có thể Malwarebytes Anti-Malware sẽ yêu cầu khởi động lại máy tính để hoàn tất quá trình.



Nếu trên màn hình xuất hiện thông báo yêu cầu khởi động lại máy tính, chỉ cần khởi động lại máy tính của bạn là xong.

Bước 4: Quét lại hệ thống bằng HitmanPro

HitmanPro tìm và loại bỏ các chương trình độc hại (malware), các chương trình quảng cáo (adware), các mối đe dọa hệ thống và thậm chí là cả virus. Chương trình được thiết kế để chạy cùng các chương trình diệt virus và các công cụ bảo mật khác.

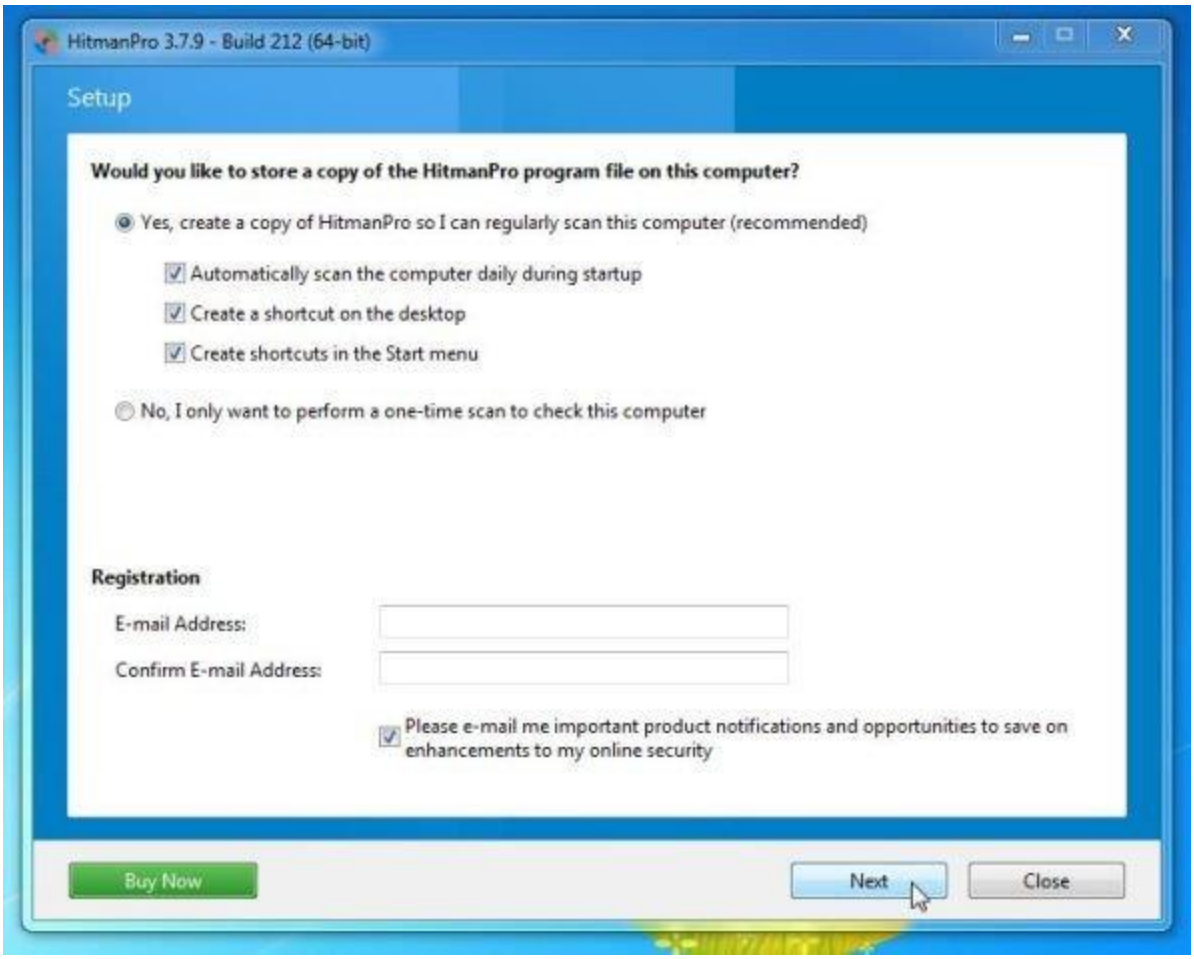
Chương trình sẽ quét máy tính của bạn với một tốc độ khá nhanh (trong vòng chưa đầy 5 phút) và không hề làm chậm máy tính của bạn như các chương trình diệt virus khác.

1. Tải HitmanPro về máy và cài đặt.

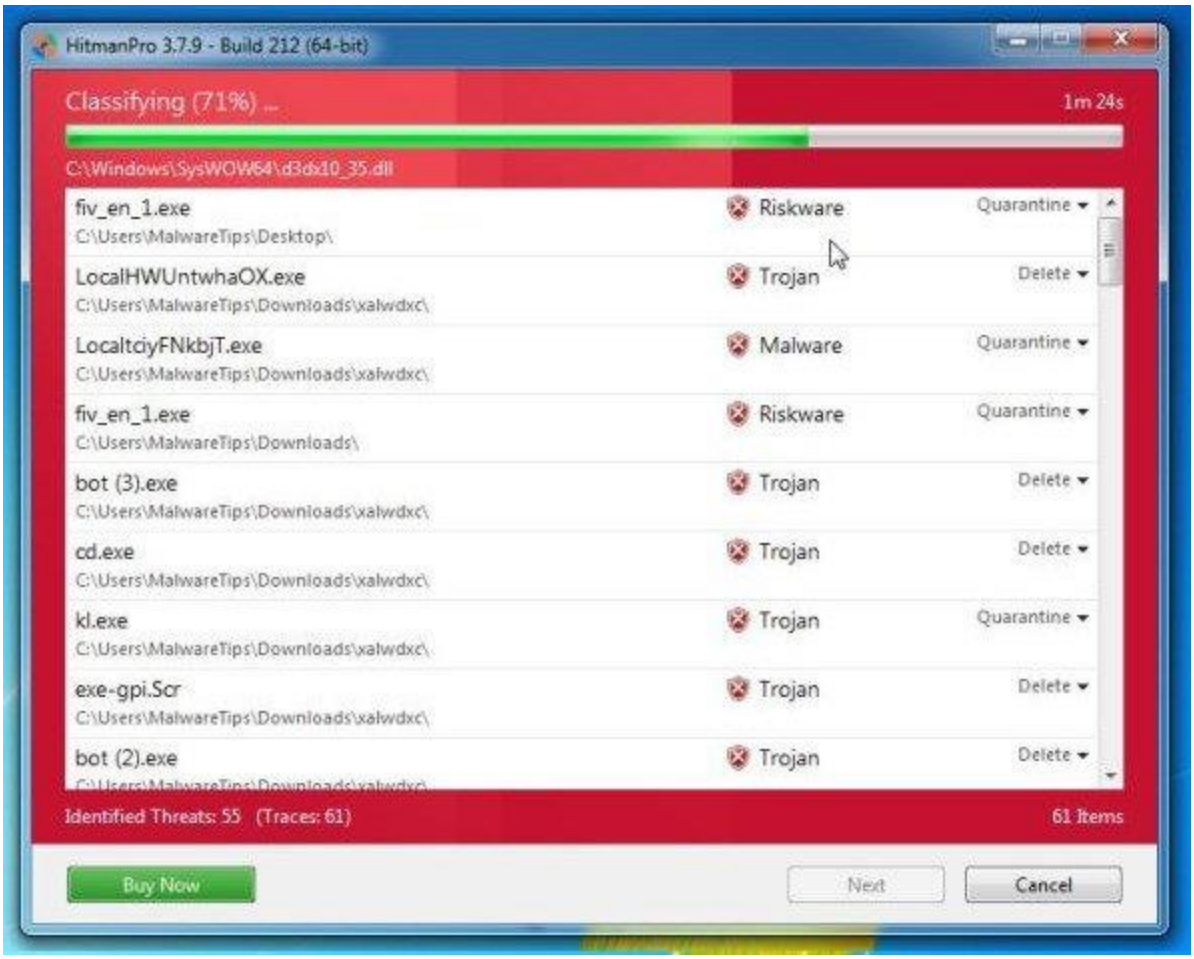
2. Kích đúp chuột vào file có tên “HitmanPro.exe” (nếu sử dụng phiên bản 32-bit) hoặc kích đúp chuột vào file “HitmanPro_x64.exe” (nếu sử dụng

phiên bản 64-bit). Khi chương trình khởi chạy, trên màn hình sẽ xuất hiện cửa sổ như hình dưới đây:

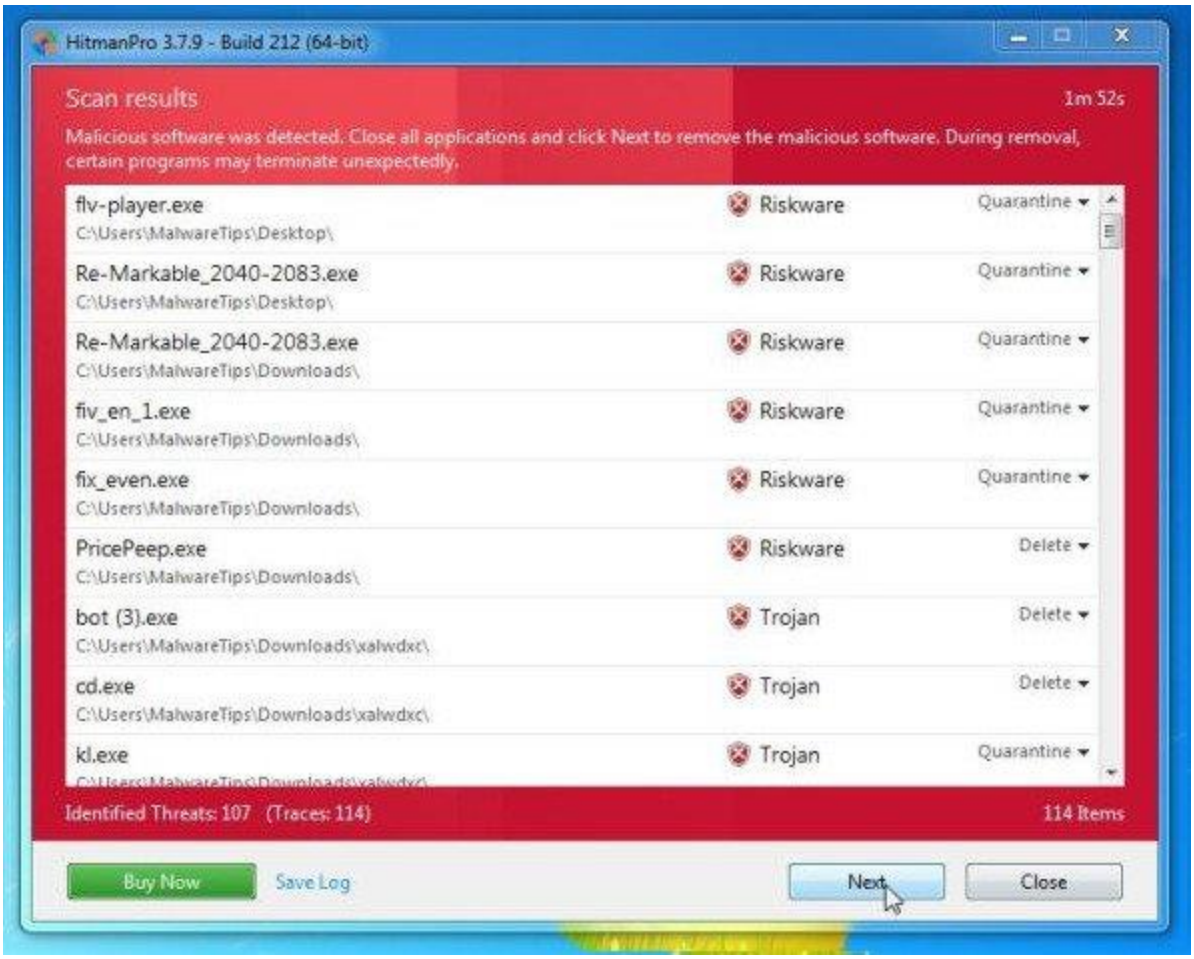
Click chọn **Next** để cài đặt HitmanPro trên máy tính của bạn.



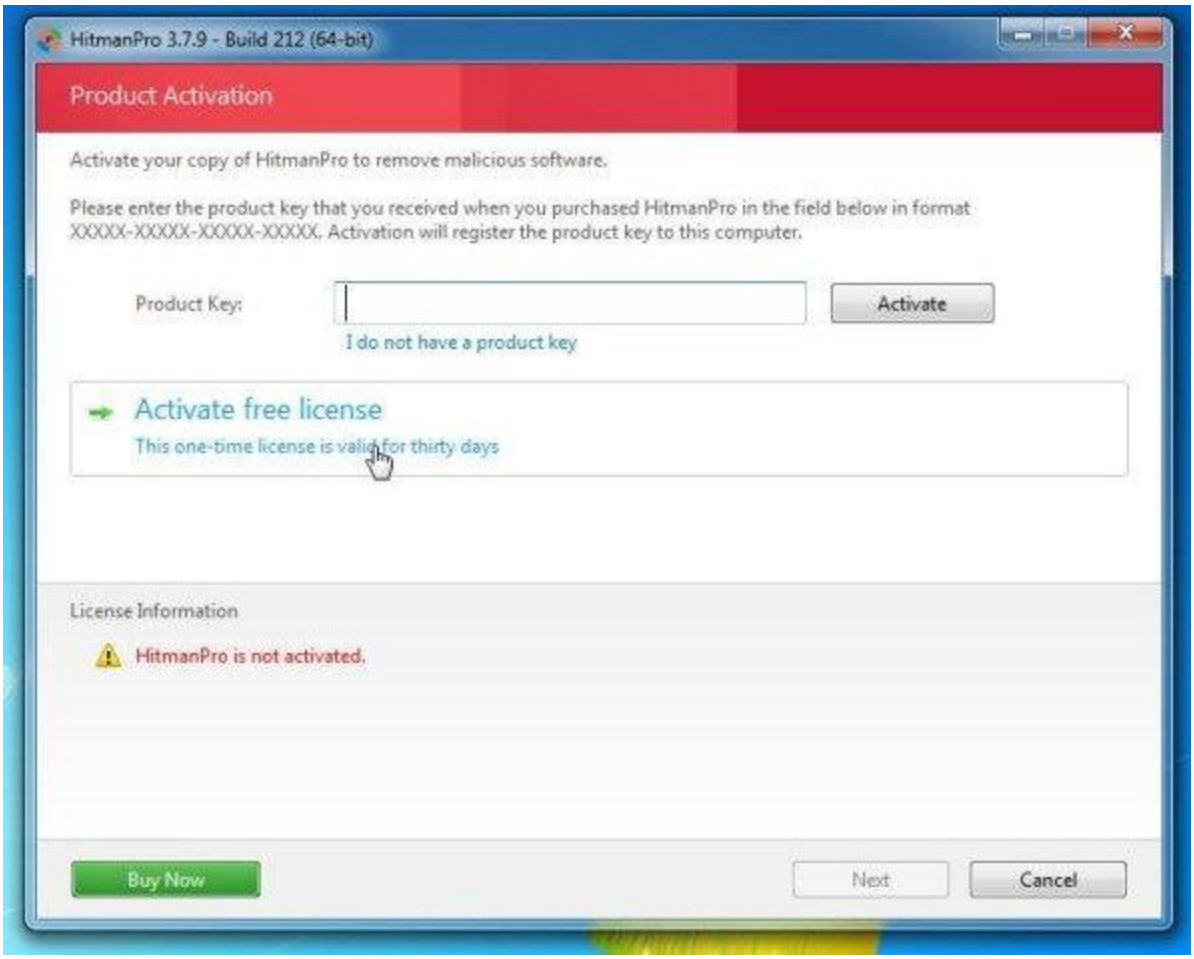
3. Và HitmanPro sẽ bắt đầu quá trình quét các tập tin độc hại HulaToo khỏi máy tính của bạn.



4. Sau khi quá trình kết thúc, HitmanPro sẽ hiển thị danh sách các chương trình độc hại (malware) mà nó phát hiện được trên hệ thống của bạn. Click chọn **Next** để gỡ bỏ các chương trình độc hại cũng như virus HulaToo đi.



5. Click chọn nút **Activate free license** để dùng thử HitmanPro trong 30 ngày và để gỡ bỏ các tập tin độc hại khỏi hệ thống của bạn.



Bước 5: Reset trình duyệt Internet Explorer, Firefox và Chrome về thiết lập mặc định ban đầu

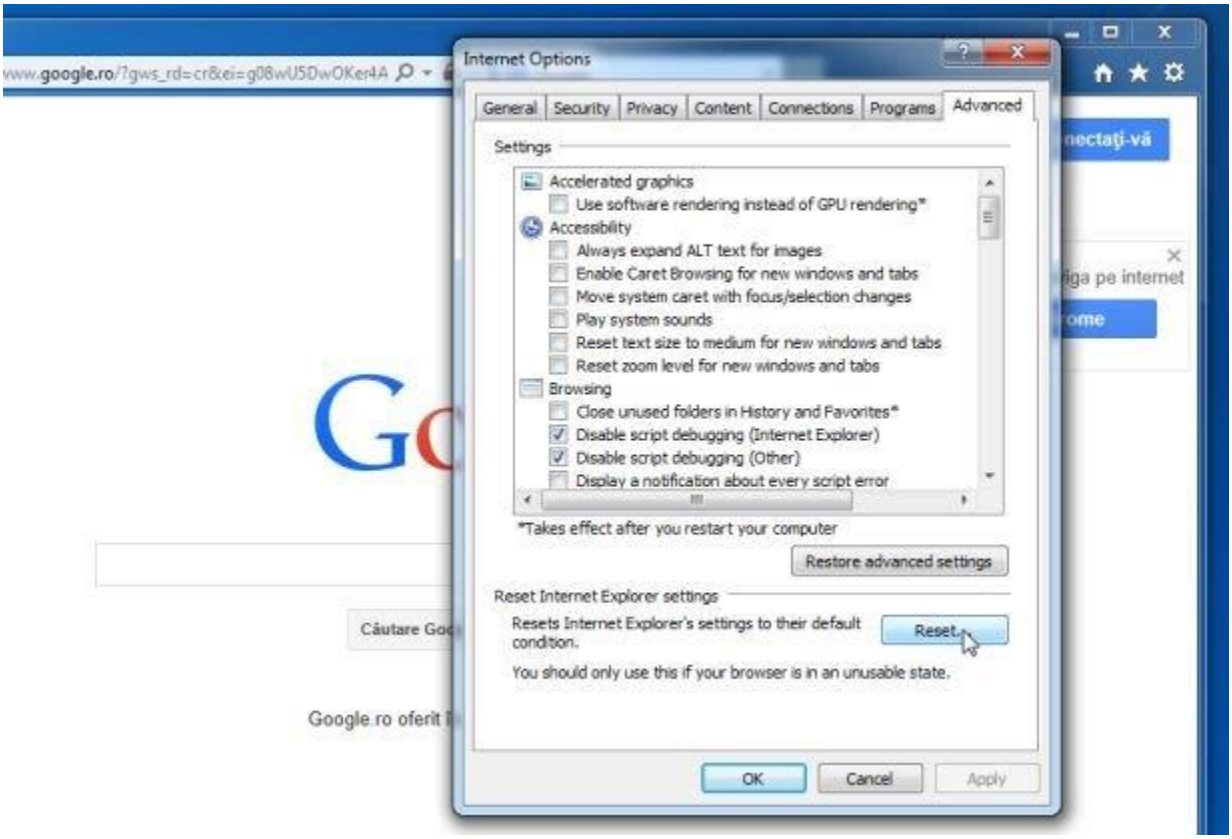
Để loại bỏ tận gốc HulaToo khỏi trình duyệt Internet Explorer, Firefox, Google Chrome và Microsoft Edge bạn sẽ phải reset lại trình duyệt về trạng thái thiết lập mặc định ban đầu.

- Trình duyệt Internet Explorer:

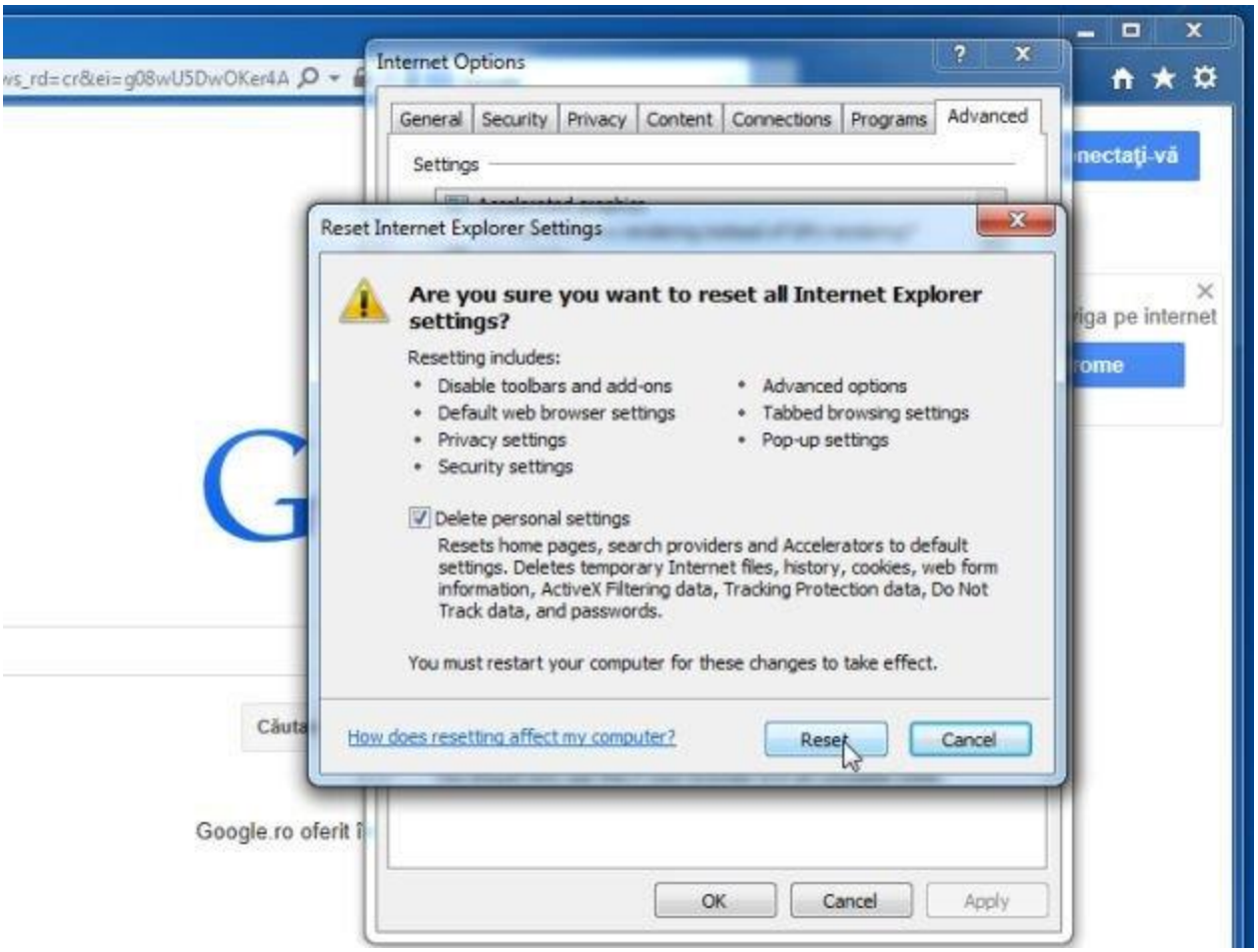
Bạn có thể reset trình duyệt Internet Explorer về trạng thái thiết lập mặc định ban đầu. Để làm được điều này:

1. Mở trình duyệt Internet Explorer trên máy tính của bạn sau đó click chọn biểu tượng hình răng cưa ở góc trên cùng bên phải màn hình, chọn Internet Options.

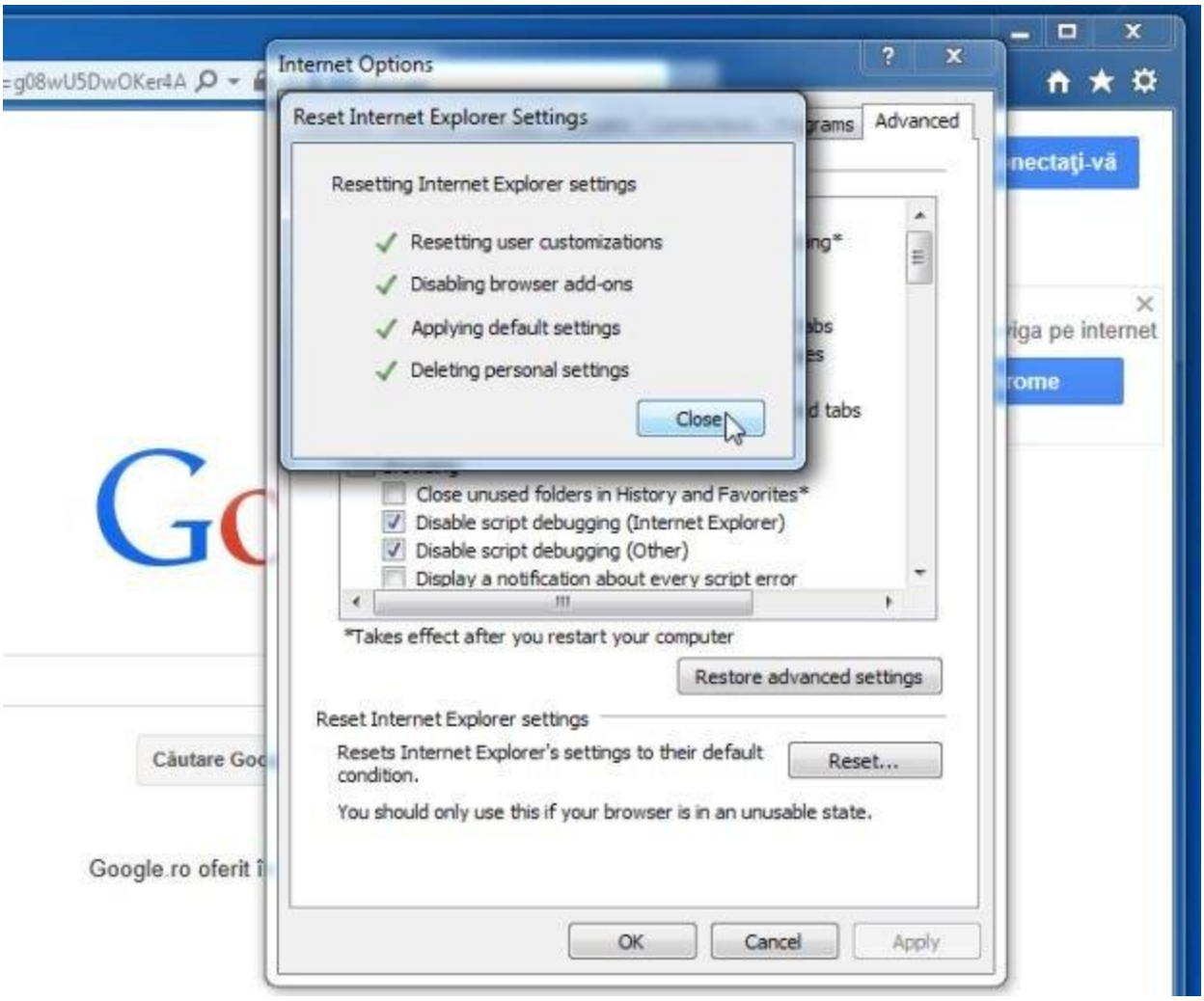
2. Trên cửa sổ hộp thoại Internet Options, click chọn **tab Advanced** rồi click chọn nút **Reset**.



3. Tiếp theo trên cửa sổ Reset Internet Explorer settings, đánh tích chọn Delete personal settings rồi click chọn nút Reset.



4. Sau khi kết thúc quá trình, click chọn nút **Close** trên hộp thoại xác nhận.

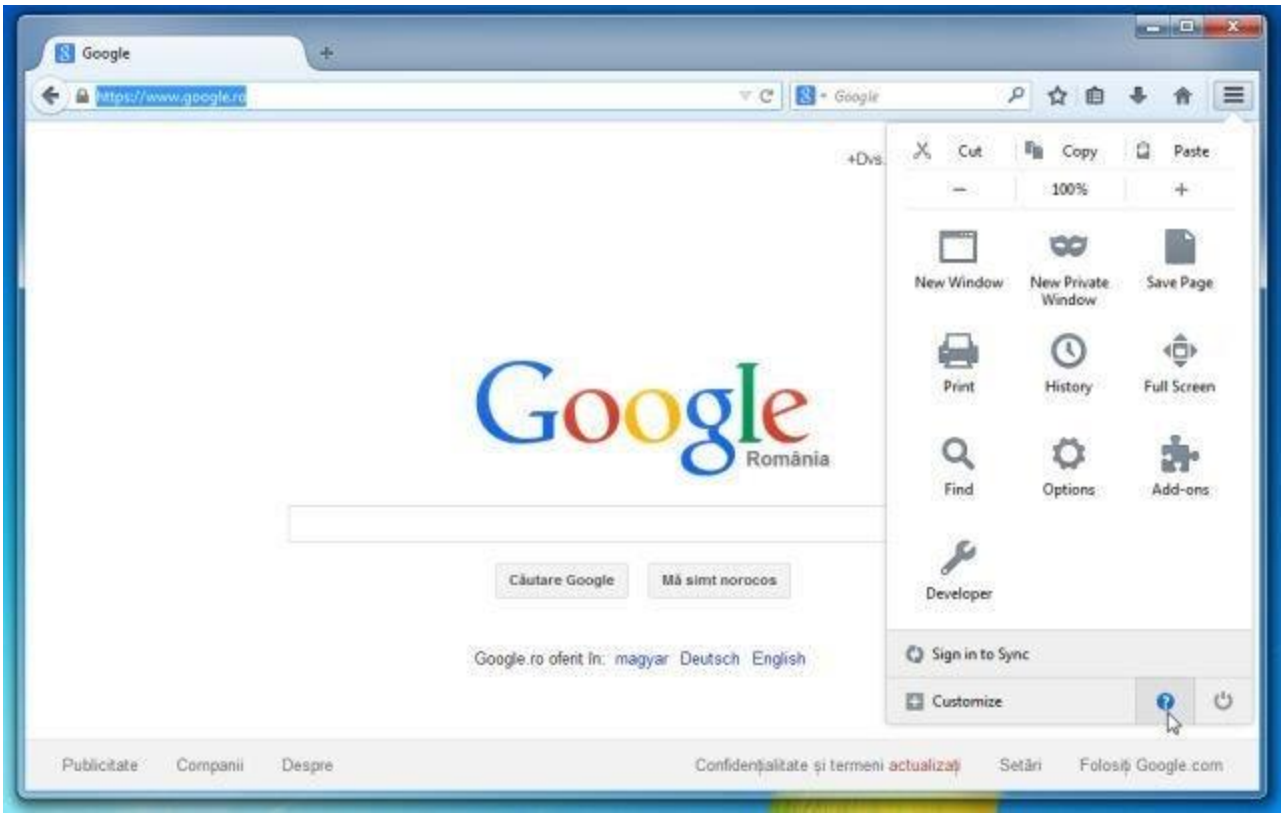


Trình duyệt Firefox:

Quá trình reset trình duyệt Firefox sẽ không làm mất các thông tin quan trọng mà bạn đã lưu trên trình duyệt như mật khẩu, bookmark, tự động điền thông tin, lịch sử duyệt web và mở các tab.

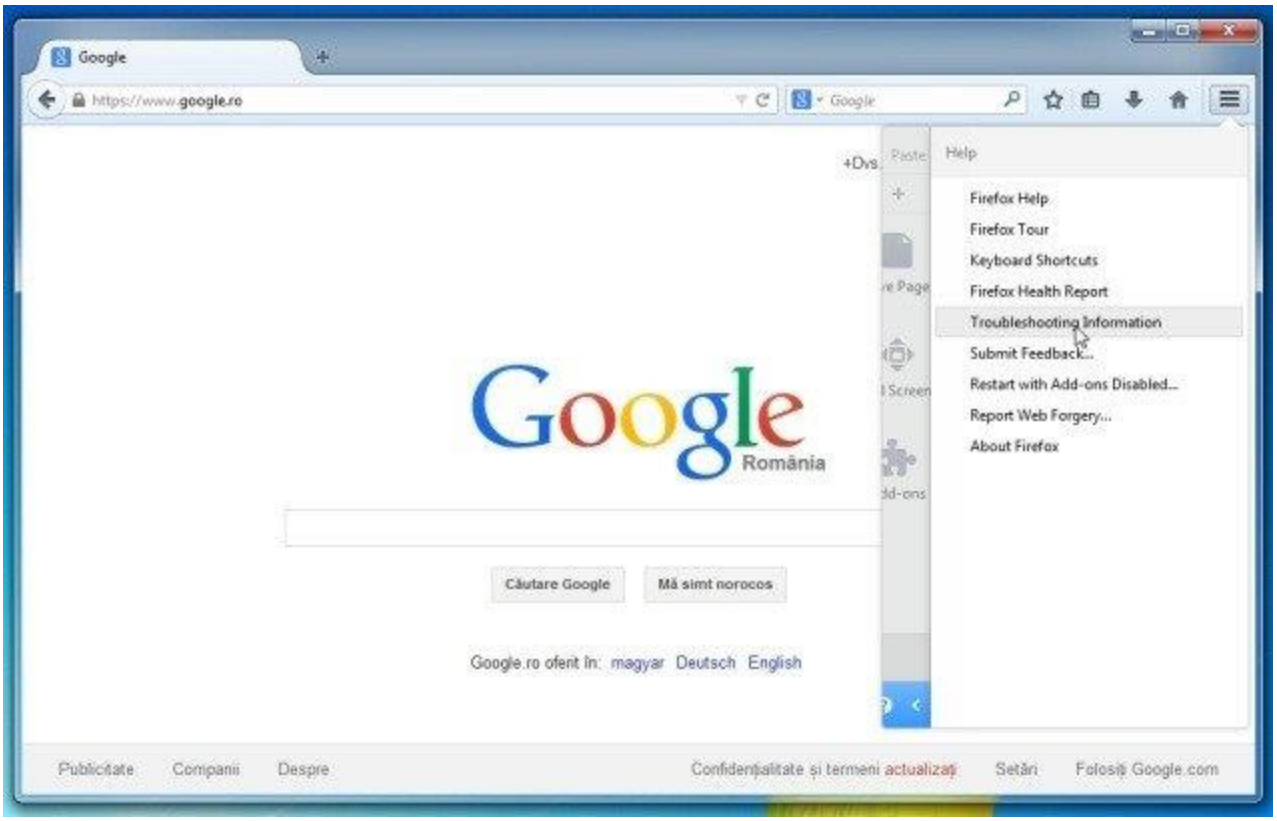
Để reset trình duyệt Firefox về trạng thái mặc định ban đầu, bạn thực hiện theo các bước dưới đây:

1. Mở trình duyệt Firefox trên máy tính của bạn, sau đó click chọn biểu tượng 3 dòng gạch ngang ở góc trên cùng bên phải màn hình, click chọn nút **Help**.

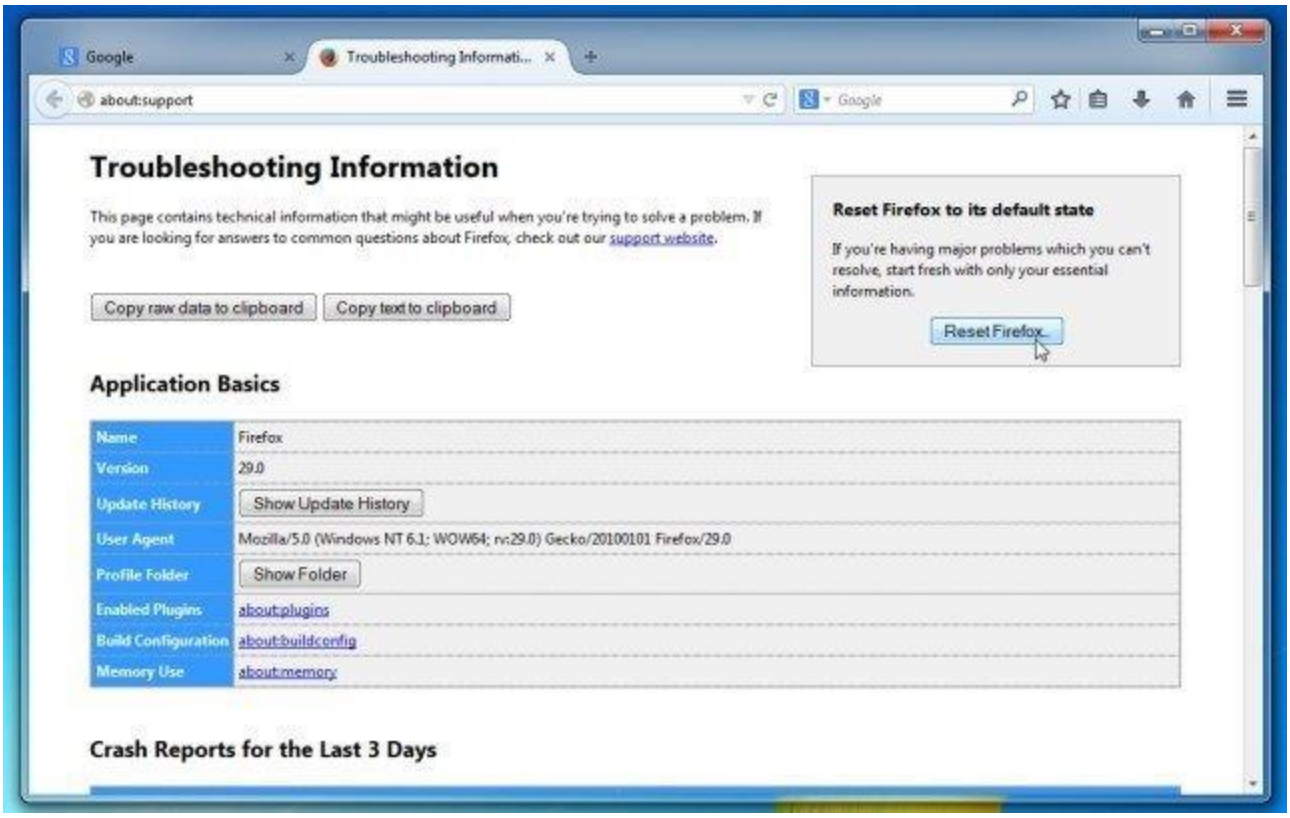


2. Từ Menu Help, chọn **Troubleshooting Information**.

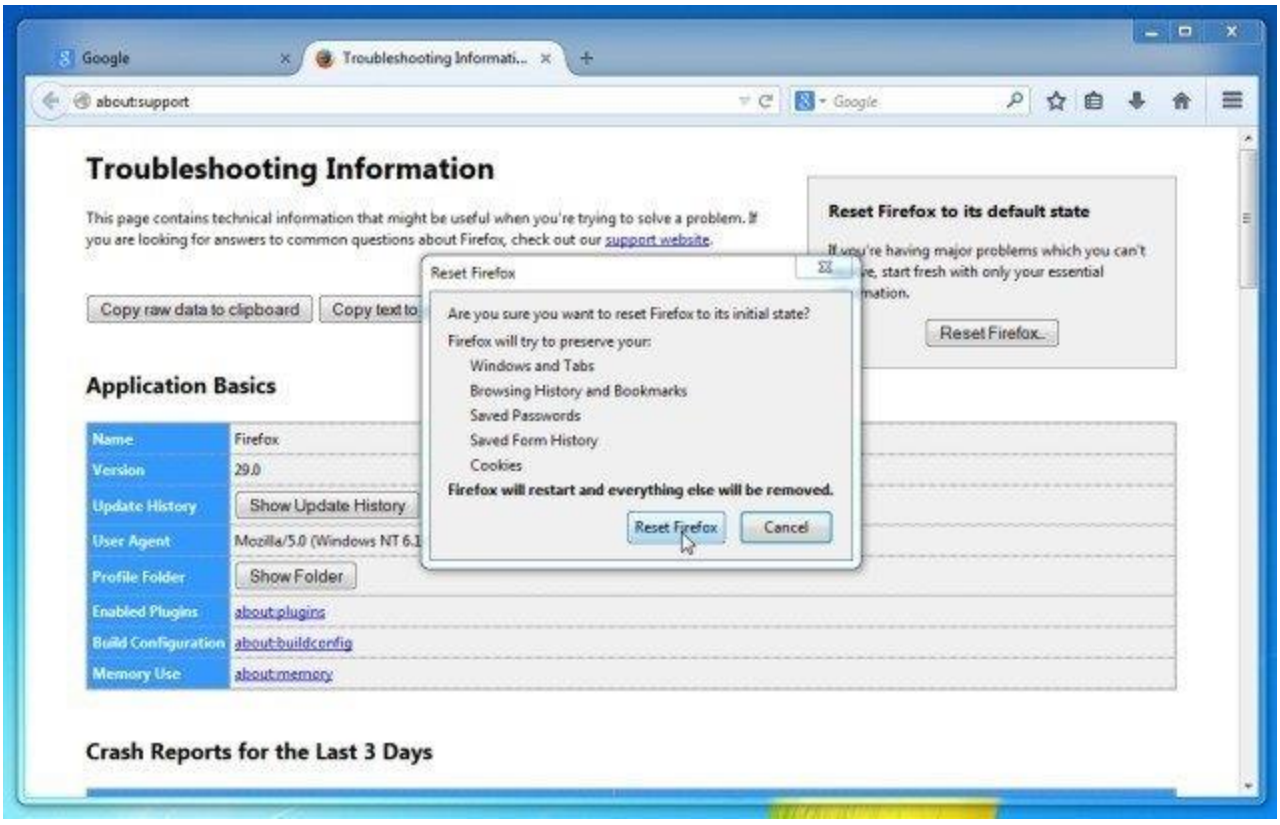
Nếu không thể truy cập Menu Help, bạn nhập **about:support** vào thanh địa chỉ rồi nhấn Enter để mở trang Troubleshooting Information.



3. Click chọn nút **Refresh Firefox** ở góc trên cùng bên phải trang Troubleshooting Information.



4. Để tiếp tục, click chọn nút **Refresh Firefox** trên cửa sổ xác nhận.

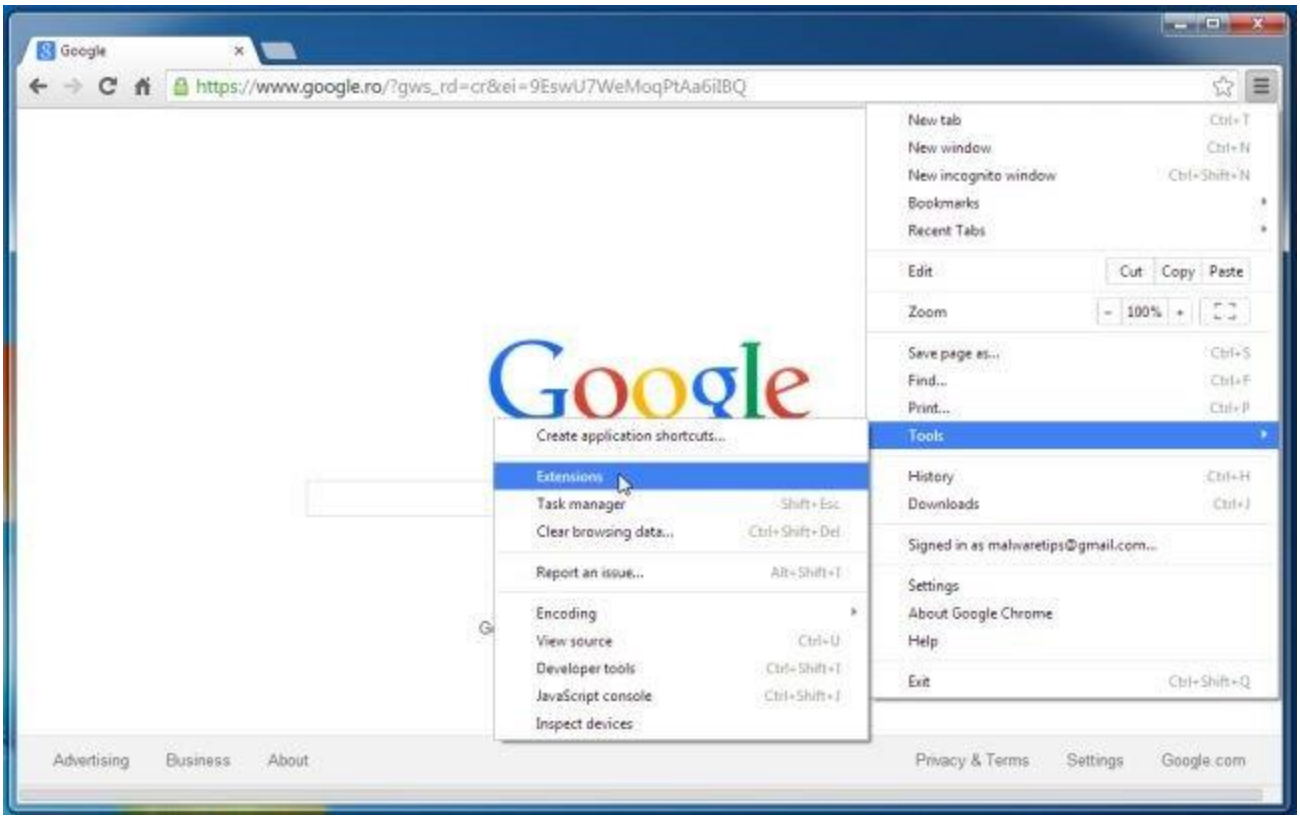


5. Firefox sẽ tự đóng lại và chuyển về trạng thái thiết lập mặc định ban đầu. Sau khi hoàn tất một cửa sổ hiển thị các thông tin đã được chuyển đổi xuất hiện. Bạn click chọn Finish là xong.

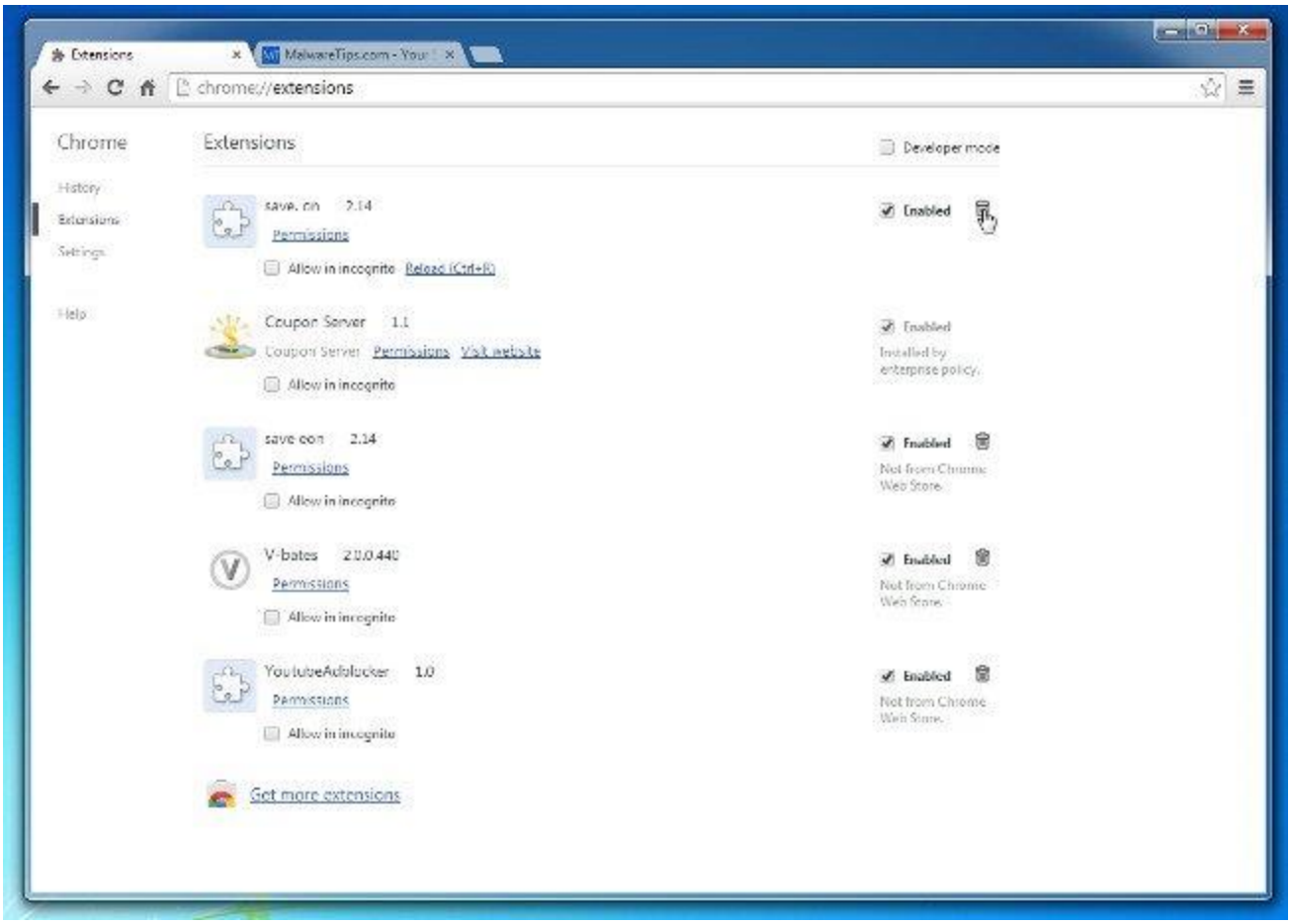
- Trình duyệt Chrome:

Google Chrome tích hợp tùy chọn reset trình duyệt về trạng thái thiết lập mặc định ban đầu. Việc reset thiết lập trình duyệt sẽ reset lại các thay đổi không mong muốn gây ra bởi việc cài đặt các chương trình khác trên hệ thống. Tuy nhiên mật khẩu và bookmark mà bạn lưu sẽ bị xóa sạch.

1. Trên trình duyệt Chrome, click chọn biểu tượng 3 dòng gạch ngang hoặc 3 dấu chấm ở góc trên cùng bên phải màn hình, sau đó click chọn **Extensions**.



2. Trên cửa sổ **Extensions**, tìm và xóa bỏ tiện ích mở rộng Hula Too và các tiện ích mở rộng không rõ nguồn gốc bằng cách click chọn biểu tượng thùng rác.


Extensions
MalwareTips.com - Your
chrome://extensions
Chrome
History
Extensions
Settings
Help
Extensions
Developer mode
save. on 2.14
Permissions
Allow in incognito
Reload (Ctrl+R)
Enabled
Coupon Server 1.1
Coupon Server
Permissions
Visit website
Allow in incognito
Enabled
Installed by enterprise policy.
save con 2.14
Permissions
Allow in incognito
Enabled
Not from Chrome Web Store.
V-bates 2.0.0.440
Permissions
Allow in incognito
Enabled
Not from Chrome Web Store.
YouTubeAdblocker 1.0
Permissions
Allow in incognito
Enabled
Not from Chrome Web Store.
Get more extensions