HƯỚNG DẪN KIỂM TRA VÀ PHÁT HIỆN PHẦN MỀM MÃ ĐỘC "ĐÀO" TIỀN ẢO BẤT HỢP PHÁP

1. Đối với quản trị website: cần kiểm tra, rà soát mã nguồn để phát hiện các mã được chèn vào. Dấu hiệu nhận biết gồm các từ khóa trong mã nguồn website "coinhive.com", "coinhive", "coin-hive", "coinhive.min.js", "authedmine.com", "authedmine.min.js.

- Bước 1: Đăng nhập vào trang web của đơn vị - Click chuột phải chọn View Page Source
- Bước 2: Bấm tổ hợp phím Ctrl + F và tìm lần lược các từ khóa ở trên.

Nếu phát hiện website bị chèn các mã khai thác như đã nêu trên, cần rà soát và kiểm tra lại lỗ hổng trên máy chủ, lỗ hổng trên website, kiểm tra các tài khoản bị lộ lọt có quyền thay đổi mã nguồn, nhằm khắc phục lỗ hổng bị lợi dụng.

2. Đối với quản trị mạng:

Triển khai các biện pháp nhằm ngăn chặn việc chạy các đoạn mã trái phép "Coinhive" trên máy tính như sau:

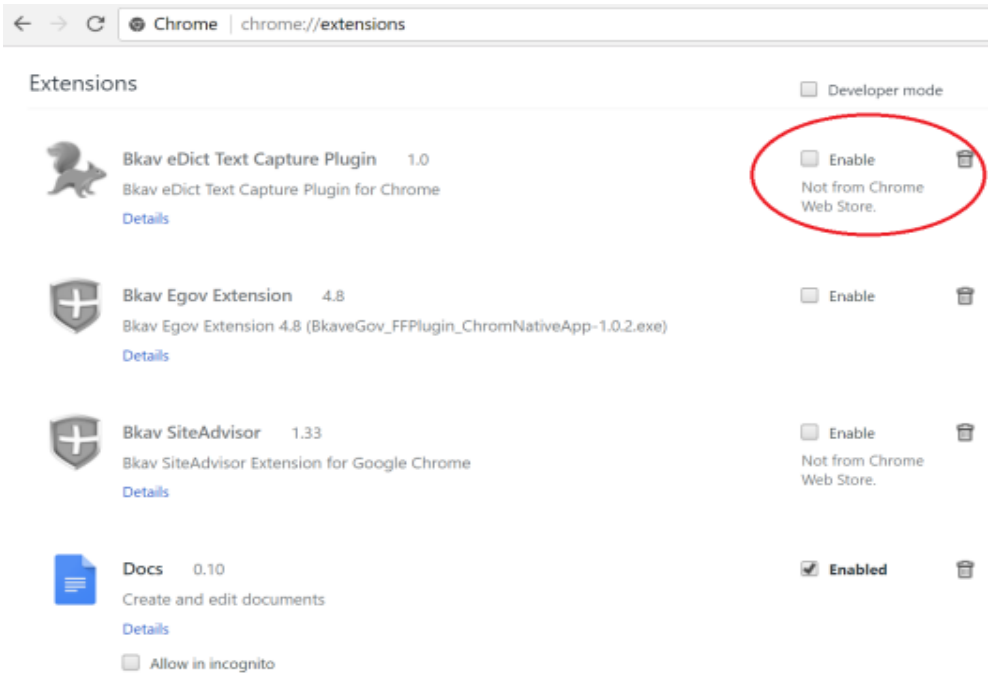
- Thực hiện giám sát và bóc gỡ xử lý trên các máy tính trong mạng có xuất hiện các kết nối đến các địa chỉ tên miền sau: afminer.com, coin-have.com, coinerra.com, coinhive.com, coinnebula.com, crypto-loot.com, hashforcash.us, jescoin.com, ppoi.org, authedmine.com;

- Sử dụng tường lửa để chặn các kết nối ra các địa chỉ sau:afminer.com, coin-have.com, coinerra.com, coinhive.com, coinnebula.com, crypto-loot.com, hashforcash.us, jescoin.com, ppoi.org, authedmine.com;

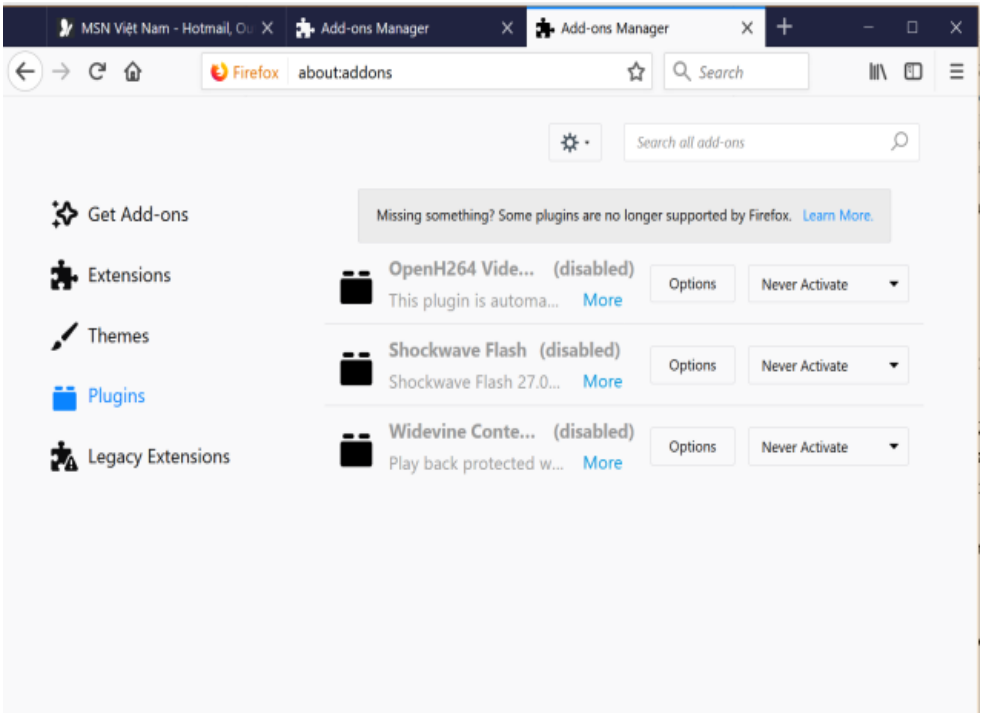
- Rà quét, kiểm tra hệ thống để tìm ra và loại bỏ các đoạn mã có trong các phần mềm mở rộng "Add-on" của trình duyệt web;

Các thực hiện:

+ Đối với trình duyệt Chrome: click vào thanh địa chỉ gõ **chrome://extensions/** kiểm tra xem có Add-on bất thường nào không, nếu có thì click chọn **Disable** hoặc **Remove** Add-on

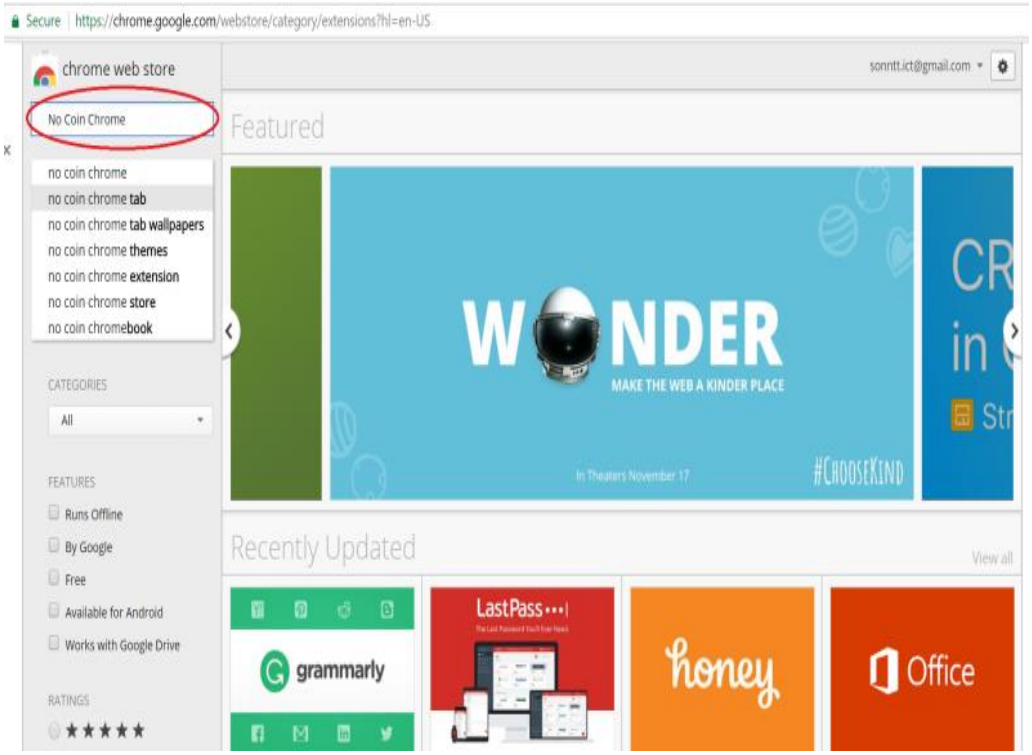


+ Đối với trình duyệt Firefox: click vào thanh địa chỉ gõ **about:addons** kiểm tra xem có Add-on bất thường nào không, nếu có thì click chọn **Disable** hoặc **Remove** Add-on

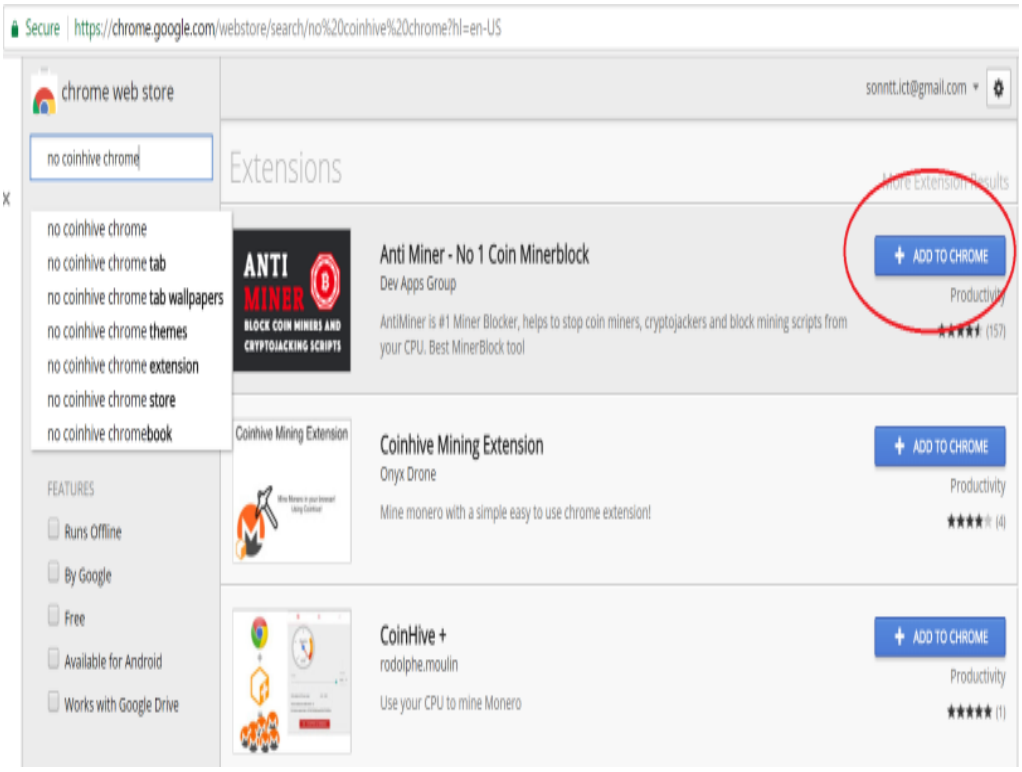


- Hướng dẫn người dùng cài đặt các tiện ích mở rộng: "No Coin Chrome" hay "minerBlock" đối với Chrome; cài đặt "No Scripts" cho Firefox.

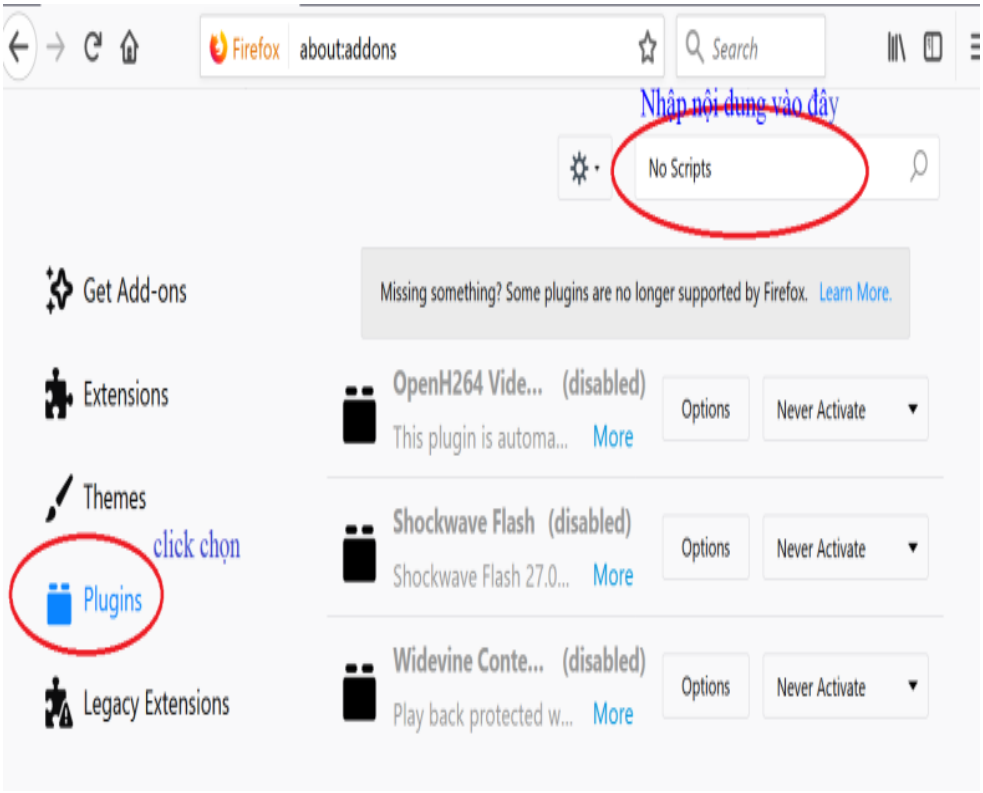
+ Đối với Chrome: click vào thanh địa chỉ gõ đường dẫn: https://chrome.google.com/webstore/category/extensions?hl=en-US ngay hộp thoại tìm kiếm đánh "**No Coin Chrome**"



Click Add to Chrome để thêm Add-on "No coin Chrome" vào trình duyệt Chrome



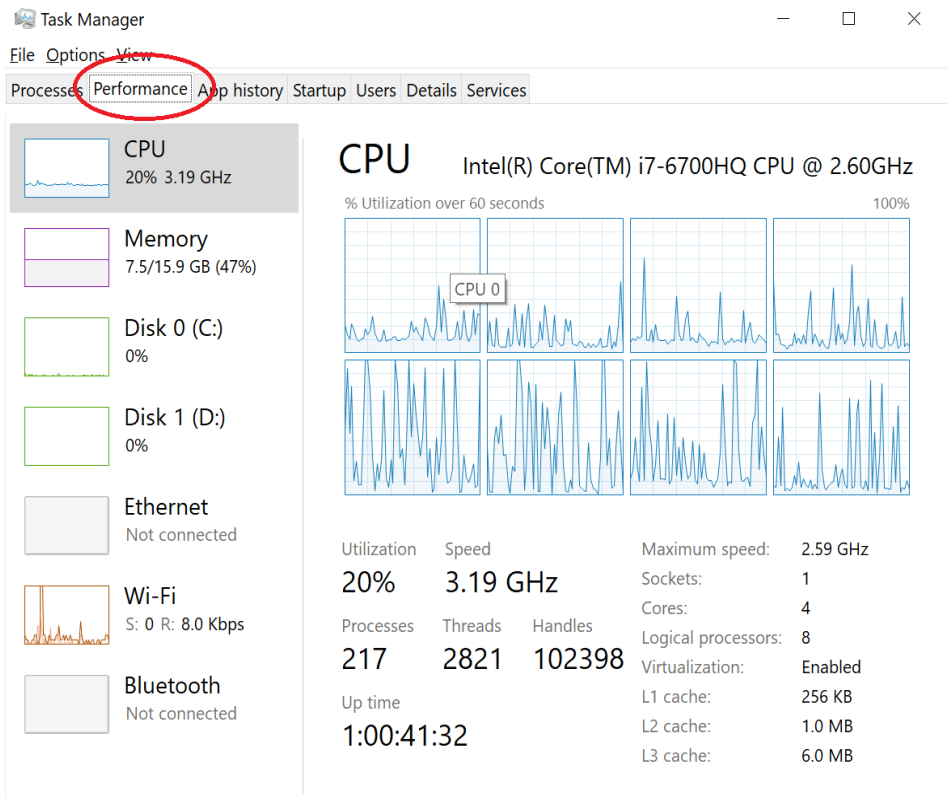
+ Đối với Firefox: click trên thanh địa chỉ của trình duyệt Firefox gõ vào đường dẫn: **about:addons** click qua thẻ **Plugins** ngay hộp thoại tìm kiếm đánh "**No Scripts**"



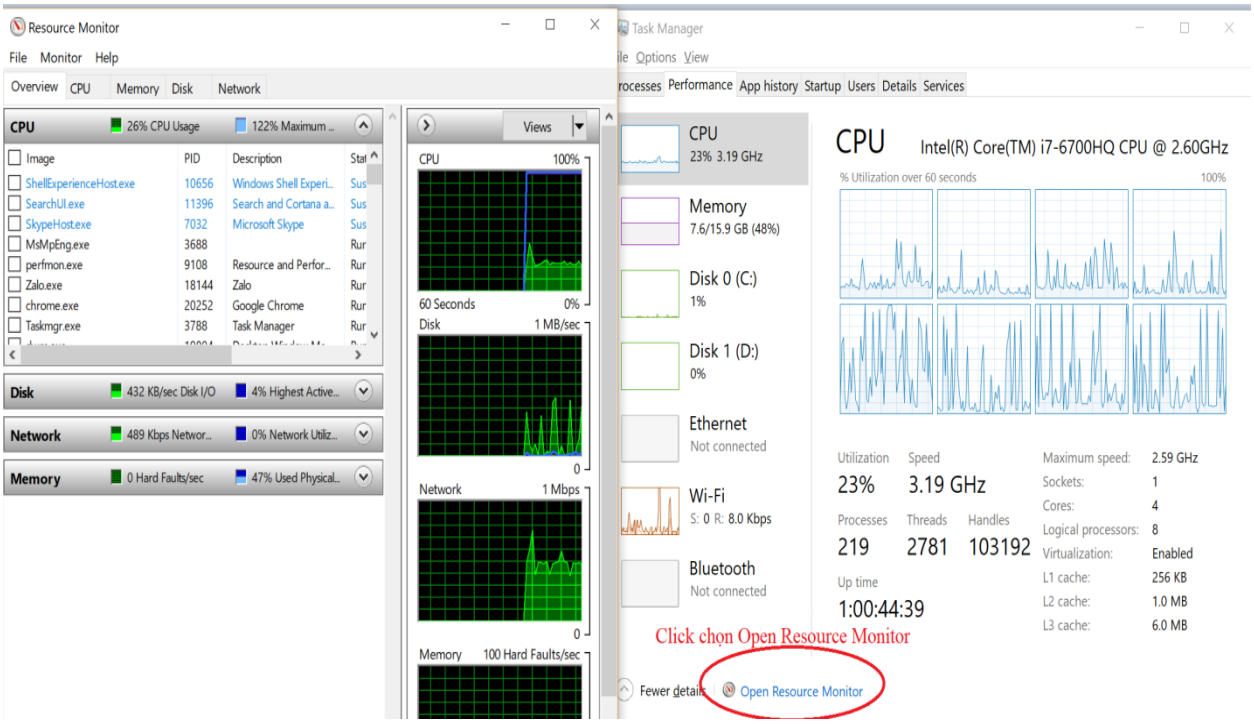
3. Hướng dẫn người dùng kiểm tra hiệu suất sử dụng CPU của máy tính bằng các ứng dụng như Windows Task Manager và Resource Monitor. Nếu máy có dấu hiệu chậm chạp và kiểm tra thấy hiệu suất sử dụng CPU của trình duyệt hoặc tiện ích mở rộng cao thì có thể máy tính đó đã bị nhiễm Coinhive. Cần thông báo gấp cho quản trị mạng để xử lý.

Cách thực hiện:

Bước 1: Click vào thanh **Taskbar** chọn **Task Manager** -> click chọn thẻ **Performance** để xem hiệu xuất sử dụng của máy tính



Bước 2: Click chọn **Open Resource Monitor** thử thẻ **Task Manager** để xem hiệu năng của máy tính



4. Thường xuyên kiểm tra và quét các lỗ hổng tồn tại trên hệ thống để phát hiện kịp thời sự xuất hiện của các đoạn mã độc hại. Trong trường hợp phát hiện ra các lỗ hổng, lập tức triển khai biện pháp khắc phục, cập nhật các bản vá bổ sung và loại bỏ các chương trình độc hại đã bị tin tặc chèn vào