Tất tần tật những điều bạn cần biết về adware (phần mềm quảng cáo)

Bạn vào mạng Internet nhưng liên tục bị làm phiền bởi những trang web quảng cáo không lành mạnh cứ tự động bật ra (pop-up) giữa màn hình? Trang chủ (Home Page) của bạn tự nhiên bị thay bằng một trang web không rõ ở đâu ra?

Bạn tìm cách loại bỏ chúng bằng cách đặt lại trang chủ của trình duyệt Internet Explorer, khôi phục lại toàn bộ những thông số mặc định của trình duyệt (Restore Defaults) hay nếu bạn là một người thông thạo về máy tính, bạn đã tìm và tắt toàn bộ những chương trình được nạp lúc khởi động… Nhưng cũng chẳng có tác dụng gì, chúng vẫn như những "con ma" lẩn trốn và tiếp tục bám dai dẳng trên máy tính của bạn. Bạn tự hỏi, thật ra những "con ma" đó là gì và tại sao chúng lại có thể "chui vào" máy tính của mình từ lúc nào không hay? Đây chính là những biểu hiện của PC nhiễm Adware. Vậy Adware là gì, có những loại adware nào và làm sao để khắc phục khi bị nhiễm adware? Chúng ta sẽ cùng tìm hiểu trong bài viết này nhé.

Adware là gì?

Adware là phần mềm không mong muốn được thiết kế để xuất hiện quảng cáo trên màn hình thiết bị của bạn, thường trong trình duyệt web. Một số chuyên gia bảo mật xem nó là tiền thân của những chương trình không mong muốn PUP (Potentially Unwanted Program). Thông thường, nó sử dụng một phương pháp lén lút để ngụy trang trở nên hợp pháp và đi kèm với một chương trình khác để lừa người dùng tải nó về máy tính để bàn, máy tính bảng hoặc thiết bị di động.

Adware mang lại lợi nhuận cho nhà phát triển của nó bằng cách tự động hiển thị quảng cáo online trong giao diện người dùng của phần mềm hoặc trên màn hình trong quá trình cài đặt. Và khi đó bạn sẽ thấy các chương trình giảm cân siêu tốc, cung cấp bí quyết làm giàu nhanh chóng và thậm chí là những cảnh báo virus giả mạo "mời" bạn click vào. Ngoài ra bạn có thể thấy các tab mới tự động mở, thay đổi trang chủ trình duyệt, kết quả từ công cụ tìm kiếm bạn chưa thấy bao giờ hoặc thậm chí chuyển hướng đến trang khác.

Điều này xảy ra khi các ứng dụng phần mềm hợp pháp sử dụng quảng cáo trực tuyến với các quảng cáo thường được gói trong chương trình và hiển thị theo cách các nhà phát triển chương trình chỉ định. Bạn có thể tải adware về máy tính mà không hề hay biết, vì nó giấu mình trong các phần mềm hợp pháp. Và bạn sẽ thấy một số chương trình máy tính hiển thị những quảng cáo không đến từ các trang web bạn đang truy cập.

Khi adware xâm nhập vào thiết bị của bạn, nó có thể thực hiện tất cả các loại tác vụ không mong muốn. Chức năng của phần mềm có thể được thiết kế để phân tích vị trí và trang web bạn truy cập, sau đó hiển thị quảng cáo phù hợp với loại hàng hóa hoặc dịch vụ bạn xem. Mặc dù adware gây phiền toái nhiều hơn là đe dọa tới an ninh mạng của bạn như phần mềm độc hại, nhưng nếu nhà phát triển adware bán

các hoạt động duyệt web và thông tin của bạn cho bên thứ ba, họ thậm chí có thể sử dụng nó để nhắm vào bạn nhiều quảng cáo hơn tùy theo thói quen duyệt web của bạn. Và dù bạn sử dụng trình duyệt web nào đi nữa như Chrome, Firefox, v.v… nó đều xuất hiện quảng cáo.

Dưới đây là một vài dấu hiệu điển hình cho thấy hệ thống của bạn có adware:

- Quảng cáo xuất hiện ở những nơi nó không nên xuất hiện.
- Trang chủ của trình duyệt web đã thay đổi một cách bí ẩn mà không có sự cho phép của bạn.
- Các trang web bạn thường truy cập không hiển thị đúng cách.
- Liên kết trang web chuyển hướng đến các trang web khác không đúng ý bạn.
- Trình duyệt web bị chậm.
- Thanh công cụ, extension hoặc plugin mới đột nhiên xuất hiện trên trình duyệt.
- Máy Mac bắt đầu tự động cài đặt các ứng dụng phần mềm không mong muốn.
- Trình duyệt bị treo.

Làm thế nào adware "chui" vào hệ thống của bạn?

Có hai cách chính adware sử dụng để xâm nhập vào hệ thống của bạn. Cách thức đầu tiên là bạn tải chương trình thường là phần mềm miễn phí (freeware) hoặc phần mềm dùng thử trước khi mua (shareware) và nó sẽ yên lặng cài đặt adware mà không có sự cho phép của bạn. Đó là bởi vì các nhà phát triển chương trình đã đăng ký với nhà cung cấp phần mềm quảng cáo. Người dùng muốn sử dụng phần mềm miễn phí thì phải chấp nhận quảng cáo (mặc dù ngay cả phần mềm trả phí từ nguồn không đáng tin cậy có thể có adware trong đó).

Cách thức thứ hai là khi bạn truy cập vào trang web bị nhiễm adware, lợi dụng lỗ hổng trình duyệt web, adware sẽ được tải xuống ổ đĩa. Sau khi chui vào hệ thống, adware bắt đầu thu thập thông tin của bạn, chuyển hướng đến trang web độc hại và ném nhiều quảng cáo hơn vào trình duyệt.

Các loại adware phổ biến

Bằng các cách trên adware đã thâm nhập vào máy tính hoặc các thiết bị khác của bạn, nó thay đổi trình duyệt web mà người dùng không biết hoặc không đồng ý. Thông thường nó sẽ thay đổi trang chủ và cài đặt tìm kiếm mặc định. Khi lướt web thấy xuất hiện các quảng cáo, bạn sẽ cho rằng nó xuất hiện từ trang web bạn truy cập nhưng không phải vậy, nó có thể từ hệ thống của bạn.

Có một số adware cho các thiết bị và hệ điều hành khác nhau. Vì vậy bạn có thể phải đối phó với adware di động/Android, adware Mac hoặc adware Windows.

Adware trên máy Mac

Nhiều người cho rằng người dùng Mac không lo sợ adware bởi vì Mac có hệ thống anti-malware tích hợp được gọi là XProtect, một công cụ khá tốt để phát hiện các phần mềm độc hại đã biết. Thực tế, tội phạm mạng thường tập trung chủ yếu vào máy tính Windows nhưng gần đây tình trạng này đã thay đổi. Adware đặc biệt

dành cho Mac đầu tiên xuất hiện vào năm 2012 và sau đó các phiên bản adware cho Mac đã tăng nhanh, được các hacker và tội phạm có tổ chức phát triển bí mật cũng như trong các tập đoàn có vẻ hợp pháp, khẳng định bán phần mềm thật cho người dùng. Adware của các công ty này được ẩn trong một phần cài đặt của phần mềm, thường người đọc hay bỏ qua nó. Do vậy khi click vào thỏa thuận, bạn đã chấp nhận tải nó về hệ thống.

Dấu hiệu cho thấy máy Mac bị nhiễm adware cũng tương tự như trên Windows. Bạn sẽ thấy các cửa sổ quảng cáo hiện ra, đôi khi làm thay đổi trang chủ trình duyệt mà bạn không biết, điều hướng đến trang web khác. Nó thậm chí còn thay thế công cụ tìm kiếm mới. Mặc dù Mac ít bị tổn thương hơn so với Windows, nhưng nó vẫn có vấn đề với adware.

Adware trên thiết bị di động

Khi một biểu tượng bí ẩn xuất hiện trên màn hình, các đoạn quảng cáo làm "tắc nghẽn" thanh thông báo, bạn biết là mình có những "vị khách" adware "không mời mà đến" rồi đó. Không có gì bất ngờ khi hàng ngàn ứng dụng Android chứa adware.

Có hai cách thức adware có thể chui vào thiết bị di động: thông qua trình duyệt web và ứng dụng tải về.

- Adware thâm nhập vào thiết bị di động thông qua trình duyệt là do cách các trình duyệt xử lý chuyển hướng được thực thi bởi code JavaScript. Điều này khiến các cửa sổ pop up quảng cáo hiện ra. Cách tốt nhất để chặn quảng cáo pop up là sử dụng trình duyệt khác, vô hiệu hóa JavaScript hoặc cài đặt extension chặn quảng cáo. Một biện pháp khắc phục khác là quay lại trang trước hoặc xóa lịch sử, bộ nhớ cache. Bạn có thể tham khảo bài viết Hướng dẫn chặn cửa sổ Pop-up quảng cáo trên tất cả mọi trình duyệt.
- Adware lây nhiễm trên thiết bị di động của bạn thông qua phần mềm đã tải xuống. Chúng hoạt động với nhiều hình thức khác nhau, từ quảng cáo toàn màn hình trong hoặc bên ngoài ứng dụng bị nhiễm đến thông báo thiết bị, trên màn hình khóa. Thông thường, cửa hàng ứng dụng bên thứ ba thường cài đặt loại ứng dụng adware, do đó bạn nên tránh các cửa hàng ứng dụng như thế này.

Mặc dù adware là một loại sâu bệnh gây phiền nhiễu, nhưng nó không nguy hiểm như phần mềm độc hại. Nhiều ứng dụng miễn phí bạn tải về điện thoại thường có chứa nội dung quảng cáo của bên thứ ba, đây là doanh thu họ có thể thu về khi cung cấp phần mềm miễn phí cho bạn.

Lịch sử của adware

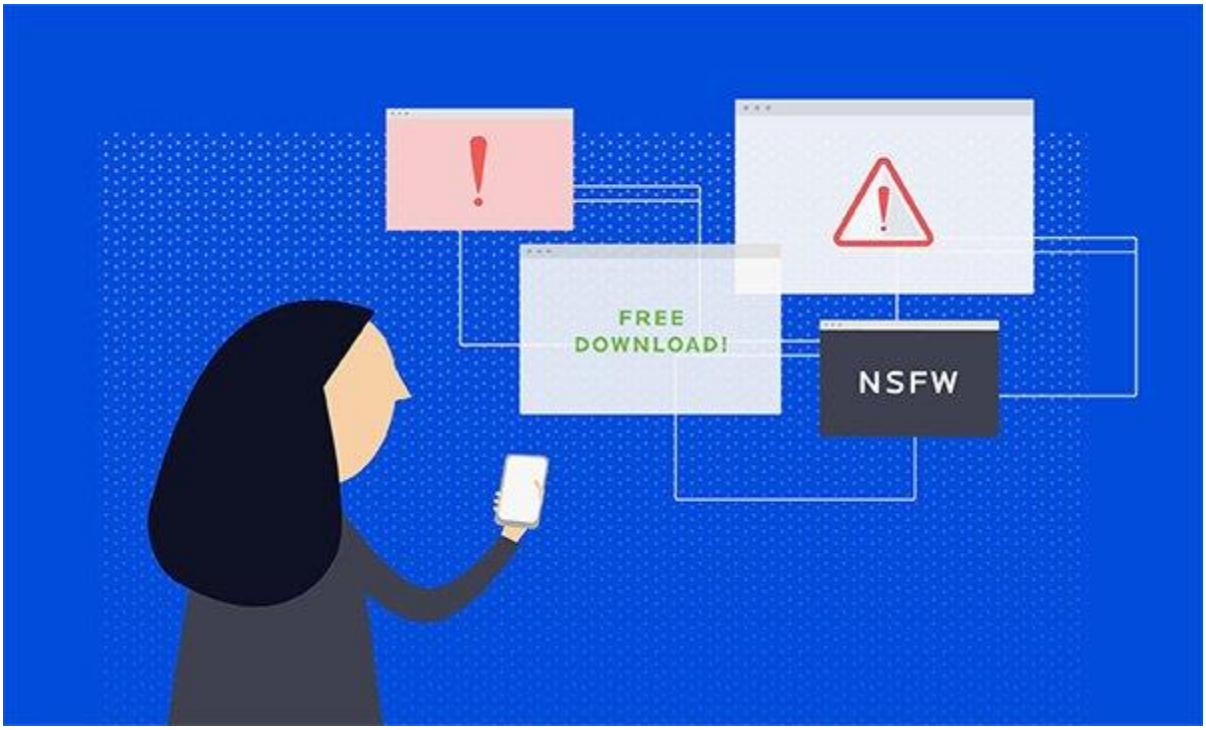
Ban đầu, khoảng năm 1995, các chuyên gia đã coi phần mềm hỗ trợ quảng cáo đầu tiên là một phần của loại spyware lớn hơn. Ngay sau đó, các chuyên gia bảo mật bắt đầu phân biệt adware với spyware như một loại PUP ít gây hại. Chúng thậm chí còn được xem là hợp pháp, ít nhất theo lý thuyết bởi vì các doanh nghiệp hợp pháp đã tạo ra phần mềm adware.

Nhưng các chi nhánh của doanh nghiệp hợp pháp này thường quảng bá adware của họ mà không được các nhà cung cấp adware kiểm tra tính hợp pháp của nó. Do việc không được kiểm tra, nên adware được tăng cường theo nhiều cách theo ý họ.

Sau một thời gian, các nhà cung cấp adware bắt đầu đóng cửa các chi nhánh có hành vi xấu và từ chối trách nhiệm đối với hành động của các chi nhánh này. Sau đó, chính quyền bắt đầu phạt tiền đối với hành vi vi phạm này, khiến những nhà phát hành adware lớn phải từ bỏ. Gần đây, những công cụ chặn quảng cáo adblocker và plugin adblock trở nên phổ biến trên trình duyệt web, chặn quảng cáo trên trình duyệt bảo vệ người dùng khỏi adware, khiến các trang web mất doanh thu từ quảng cáo hợp pháp.

Ngày nay, mặc dù adware vẫn tồn tại, nhưng nó được xem là một dạng của chương trình không mong muốn PUP với mức độ nguy hiểm thấp hơn phần mềm độc hại. Tuy nhiên adware đang hồi sinh có lẽ nhờ sự gia tăng của thiết bị di động và adware trong các ứng dụng di động. Các nhà sản xuất adware ngày nay đang củng cố quyền lực, họ sử dụng các kỹ thuật mạnh mẽ hơn như Trojian ẩn, kết hợp với các thành phần adfraud, rootkit, v.v… khiến chúng khó bị loại bỏ.

Nạn nhân của những adware này là ai?



Đối tượng chính adware nhắm tới là người dùng cá nhân. Nó theo dõi họ thông qua bất cứ con đường nào có thể từ máy tính Windows, Mac cho đến điện thoại di động và phần lớn các trình duyệt.

Cần làm gì khi bị nhiễm adware?

Nếu nghi ngờ có adware trên máy tính Mac hoặc Windows, bạn có thể thực hiện một số biện pháp để khắc phục sự cố. Tham khảo bài viết Loại bỏ hoàn toàn Adware và Spyware trên hệ thống của bạn.

Làm thế nào để bảo vệ bản thân khỏi adware?

Để tránh adware, hãy cẩn thận trước khi tải và cài đặt bất cứ phần mềm mới nào, đặc biệt là phần mềm miễn phí. Đọc điều khoản và điều kiện trước khi đồng ý. Tránh các trang web torrent, trang web download phần mềm bất hợp pháp và không bao giờ mở ứng dụng từ một nguồn không xác định, ngay cả khi nó đến với bạn dưới vỏ bọc của một liên hệ email đã biết. Cuối cùng, tải chương trình an ninh mạng uy tín cho máy tính và điện thoại di động và thực hiện quét, cập nhật thường xuyên.