Pastejacking là gì? Làm thế nào để bảo vệ máy tính của bạn khỏi Pastejacking?

Pastejacking là một phương pháp mà các trang web độc hại sử dụng để giành quyền kiểm soát clipboard trên máy tính của bạn và thay đổi các nội dung đó thành các nội dung độc hại mà bạn không hề hay biết.

1. Pastejacking là gì?

Gần như tất cả các trình duyệt đều cho phép các trang web chạy các câu lệnh trên máy tính của người dùng. Tính năng này có thể cho phép các trang web độc hại giành quyền kiểm soát clipboard trên máy tính của bạn.

Khi bạn sao chép bất kỳ một cái gì đó và dán vào clipboard, trang web có thể chạy một lệnh hoặc nhiều hơn bằng cách sử dụng trình duyệt của bạn. Phương pháp này có thể được sử dụng để thay đổi các nội dung trong Clipboard.

Ngoài ra nếu sao chép các nội dung vào Notepad hay Word… trước thì quá trình này ít nguy hiểm hơn và ít gây ra sự cố hơn là dán trực tiếp vào Command prompt.

Các trang web chạy các lệnh khi người dùng thực hiện bất cứ một hành động cụ thể nào đó, chẳng hạn như khi nhấn một phím cụ thể trên bàn phím hoặc kích chuột phải. Khi bạn nhấn tổ hợp phím Ctrl + C trên bàn phím, sẽ kích hoạt chế độ lệnh (command mode) của trang web.

Chỉ sau một khoảng thời gian ngắn, khoảng 800 mili giây nó sẽ dán các nội dụng độc hại vào clipboard của bạn. Một số trang web có thể theo dõi thao tác **CTRL + V** và sử dụng nó để kích hoạt một lệnh thay đổi nội dung trên Clipboard.

Ngoài ra các trang web có thể theo dõi các "động thái" của chuột trong trường hợp bạn không sử dụng bàn phím mà sử dụng chuột để thực hiện thao tác. Khi sử dụng menu ngữ cảnh (menu kích chuột phải) để sao chép cũng kích hoạt các lệnh để thay thế nội dung trên Clipboard.

Nói tóm lại, Pastejacking là một phương pháp mà các trang web độc hại sử dụng để giành quyền kiểm soát clipboard trên máy tính của bạn và thay đổi các nội dung đó thành các nội dung độc hại mà bạn không hề hay biết.

2. Tại sao Pastejacking lại nguy hiểm?

Giả sử bạn sao chép và dán nội dung trên một trang web nào đó vào Microsoft Word. Khi bạn nhấn tổ hợp phím **Ctrl + C** hoặc **Ctrl + V**, các trang web sẽ "gán" một số lệnh vào clipboard của bạn để tạo và thực thi Macros.

Nguy hiểm hơn là khi bạn dán các nội dung trực tiếp vào bảng điều khiển như PowerShell hoặc Command Prompt. Người dùng Mac có thể lựa chọn một số tùy chọn bảo mật nếu sử dụng iTerm.

iTerm là một mô phỏng cho phép người dùng Mac thay thế giao diện điều khiển mặc định. Khi sử dụng iTerm, nó sẽ hỏi người dùng xem họ có thực sự

muốn dán các nội dung có chứa ký tự “newline” hay không. Người dùng có thể lựa chọn Yes hoặc No, phụ thuộc vào những gì họ đang làm.

Ký tự Newline thực sự chỉ là 1/2 phím Enter. Phím Enter được mô tả bằng một phím mũi tên hướng sang trái. Phím Enter là sự kết hợp của ký tự Newline (thay đổi dòng tiếp theo) và Return.

Khi bạn nhấn phím Enter, bất kỳ một lệnh nào trên bảng điều khiển **cũng đều** được thực thi. Phụ thuộc vào giao diện điều khiển để yêu cầu xác nhận.

Trên cửa sổ Command Prompt sẽ không yêu cầu xác nhận với hầu hết các lệnh, mà chỉ yêu cầu xác nhận trong trường hợp bạn sử dụng lệnh **DEL** hoặc lệnh **FORMAT**. Đối với các lệnh như **RENAME**,…, Command prompt sẽ không yêu cầu xác nhận.

Trong bất kỳ mọi trường hợp, nếu các trang web thay thế các lệnh trên Clipboard bằng phím Enter (/n/r trong đó /n là newline và /r là return), giao diện điều khiển hoặc bất kỳ ứng dụng nào có thể chạy trực tiếp các lệnh. Nếu các lệnh này là lệnh nguy hiểm, chúng có thể “tàn phá” máy tính và hệ thống mạng của bạn.

3. Làm thế nào để tránh Pastejacking?

Nếu đang sử dụng Mac OS X, bạn có thể sử dụng mô phỏng iTerm để bảo vệ máy của mình trong trạng thái an toàn. iTerm sẽ nhắc nhở và thông báo cho bạn trong trường hợp khi có pastejacking xảy ra.

Với người dùng Windows phải kiểm tra xem các trang web đã gán gì vào clipboard trên máy tính của mình. Để làm được điều này, đầu tiên bạn dán nội dung vào Notepad. Notepad chỉ cho phép người dùng dán clipboard dưới dạng text (văn bản), do đó bạn có thể xem được mọi thứ trên clipboard. Nếu nhìn thấy những gì mà bạn đã sao chép

bạn có thể dán các nội dung đó vào bất kỳ vị trí nào mà bạn muốn. Điều này đồng nghĩa với việc bạn sẽ phải thực hiện thêm một bước, nhưng ngược lại bạn sẽ tránh được Pastejacked. Lưu ý rằng việc sử dụng Word để kiểm tra clipboard có thể gây nguy hiểm vì chương trình này sử dụng Macros.

Và tất nhiên nếu nội dung mà bạn sao chép và dán trên Notepad nhưng bạn không thể xem được định dạng, font chữ, style... điều này có nghĩa là nội dung mà bạn dán ở định dạng Plain text.

Với hình ảnh, cách tốt nhất là bạn kích chuột phải vào hình ảnh mà bạn muốn tải về hoặc sao chép về rồi chọn **Save As...** sẽ an toàn hơn việc sao chép lệnh.