PHẦN MỀM BẢO MẬT CÓ THẬT SỰ HOÀN HẢO?

Các phần mềm bảo mật được thiết kế để bảo vệ người sử dụng thoát khỏi những hiểm hoạ từ các phần mềm quảng cáo (adware) và các phần mềm gián điệp (spyware), sâu, virus... nhưng chúng cũng có những thiết lập mặc định không cho phép người dùng truy cập vào

Hầu hết các phần mềm bảo mật và các phần mềm chống spyware đều gặp phải một vấn đề: Trong thời gian các chương trình này bảo vệ hệ thống của người dùng, một số các cổng thông tin trực tuyến (news portal) có chứa cookie không thể truy cập được. Các cổng thông tin này thu lợi nhuận nhờ quảng cáo bằng cách sử dụng các cookie từ các hãng thứ ba. Vì vậy, người sử dụng đều không thể tới được những thông tin hữu ích từ các cổng thông tin này, họ đã bị "khoá cứng" trong thế giới của những bộ phần mềm bảo mật.Một chuyên gia phân tích về bảo mật của Yankee Group phát biểu: " Điều này xảy ra bởi các các phần mềm bảo mật xác định và loại bỏ các cookie, rất có thể những cookie "hiền lành" cũng bị coi như là những thành phần nguy hiểm. Quá khó khăn để phân biệt cookie hữu ích và cookie hiểm độc, bởi vậy xoá bỏ hoàn toàn các cookie luôn là phương pháp mà các chương trình bảo mật sử dụng."

Cookie là gì? Tại sao lại phải sử dụng Cookie?

Không quan tâm là bạn lướt tới đâu trong không gian rộng lớn của Internet, hầu hết các trang Web hầu như đều cài đặt các cookie trên máy tính của người dùng. Vậy, cookie là gì? Tại sao các trang Web lại thích sử dụng cookie?

Thực ra, cookie chỉ là một gói thông tin nhỏ thường được lưu trữ trong một file text mà các trang Web lưu lại trên máy của người sử dụng. Cookie lưu giữ một số thông tin để xác định bạn hoặc máy tính của bạn với máy chủ. Bất cứ khi nào bạn vào trang Web, các cookie này sẽ "thông báo" tín hiệu với máy chủ là bạn đã từng ghé thăm trang Web này.

Chính vì vậy, cookie thực sự chẳng làm hại gì cho máy tính cả. Không những không làm hại, mà cookie lại còn khá thuận tiện như lưu trữ mật khẩu và nạp các thông tin cần thiết. Mặc dù, trong một số trường hợp cookie sẽ đe doạ khả năng bị mất thông tin cá nhân, lộ mật khẩu..."Bức tường" không thể vượt qua

Một ví dụ điển hình là bản cập nhật phần mềm chống gián điệp của Symantec, đã chặn truy cập các trang thông tin trực tuyến bởi phần mềm này giới hạn các cookie từ những công ty quảng cáo. Tương tự, PC Tools, một chương trình chống spyware khá nổi tiếng trên thị trường, đã chặn hầu như toàn bộ tất cả những trang thông tin trực tuyến bởi những cookie này. Những lỗi này hầu như đều xảy ra với các PC cũng như laptop sử dụng các bộ công cụ McAfee Internet Security, Microsoft AntiSpyware, Symantec Internet Security, và ZoneLabs Internet Security.

Thông thường, người sử dụng sau khi đã mua về và cài đặt các chương trình bảo mật này chẳng quan tâm gì về những thiết lập mặc định. Những thiết lập mặc định hoàn toàn có thể chỉnh sửa để truy cập vào một số các trang Web chứa các cookie mang tính quảng cáo. Trong hầu hết các trường hợp, những cookie này thực sự chẳng gây nguy hiểm nào tới người sử dụng. Tuy nhiên, một số phần mềm bảo mật lại rất "khó tính", không cho thay đổi các thiết lập này. Chính điều này đã làm ảnh hưởng hàng triệu người sử dụng.

Hầu hết các chương trình chặn spyware đều hoạt động chặn các cookie ở mức độ cao, rất ít các phần mềm là có khả năng lọc bỏ cookie hiệu quả. Tiêu biểu là chương trình diệt spyware Ad-Aware SE Personal của Lavasoft. Ngoài khả năng loại bỏ các phần mềm spyware và adware ẩn nấp trong đĩa cứng, phần mềm này còn có tuỳ chọn cho phép tìm, lựa chọn sử dụng cũng như xoá

bỏ các cookie khả nghi.
Không giống như Ad-Aware các chương trình tiêu diệt phần mềm gián điệp, chương trình diệt virus khác thường xoá bỏ toàn bộ cookie cũng như những thành phần có khả năng là adware và spyware.
Phản hồi từ các chuyên gia và hãng cung cấp phần mềmNgược lại, một số chuyên gia bảo mật khác lại khẳng định xoá bỏ hoàn toàn cookie cũng không phải là quá tệ hại. Chuyên gia bảo mật của Forrester Research, Natalie Lambert thì lại cho rằng các phần mềm bảo mật xoá tất cả các cookie là cách tốt nhất để bảo vệ khách hàng.Lambert thừa nhận rất có thể các phần mềm bảo mật của Symantec và của các hãng khác chặn truy cập tới các trang tin tức hợp pháp. Nhưng nếu thực sự điều này xảy ra, thì hầu hết các khách hàng sẽ than phiền với các nhà cung cấp sản phẩm về điều đó: "Tôi công nhận rằng khách hàng sẽ chẳng được lợi gì khi mà các phần mềm chống gián điệp chặn các trang Web hợp pháp. Nhưng chúng ta cần tin tưởng vào các nhà cung cấp phần mềm bảo mật, họ luôn bảo vệ hệ thống máy tính theo cách an toàn nhất. Trong một trường hợp đặc biệt nào đó, các trang Web hợp pháp có thể bị chặn và các cookie sẽ bị xoá nhằm bảo vệ tối đa sự ảnh hưởng tới máy tính của người dùng."
Theo Richard Stiennon, phó giám đốc nghiên cứu của Webroot Software, một công ty cung cấp phần mềm chống gián điệp nổi tiếng, ông hoàn toàn đồng ý với ý kiến của Lambert. Ông cho rằng lỗi xoá các cookie cũng như chặn các trang Web hoàn toàn là do các nhà cung cấp các trang Web.Ông cũng phủ nhận giả thuyết về các phần mềm chống gián điệp cũng như các phần mềm chống virus đã có những thay đổi cũng như cập nhật nào đó nhằm chặn các trang Web hợp pháp, có tới 99% các nhà sản xuất phần mềm đều cùng sử dụng một phương pháp để xác định và săn lùng các spyware và adware.Lỗi thuộc về ai?
Giáo sư khoa học máy tính thuộc viện công nghệ ở Florida, James Whittaker cho rằng: "Các nhà cung cấp phần mềm bảo mật cũng giống như các bác sĩ thú y. Họ phải cố gắng băng bó những vết thương đang rỉ máu trên những con thú đáng thương. Nhưng cái mà họ cần đến ở đây không phải là giải pháp mà là cách làm thực tế. Các nhà cung cấp phần mềm cũng vậy, họ phải sáng tạo ra một cách nào đó để sửa lỗi phần mềm của họ."
Giáo sư Whittaker cũng cho rằng lỗi các phần mềm bảo mật cũng là một phần của vấn đề. Các phần mềm này chưa thực mạnh mẽ và đáng tin cậy. Hacker vẫn có thể xâm nhập từ những lỗ hổng của các phần mềm này. Các phần mềm bảo mật này cần phải nhanh chóng vá hết những lỗ hổng.Một phần trong những nguyên nhân gây lỗi là do phương pháp thiết kế các phần mềm. Với khoảng hơn 100 000 virus, sâu, spyware, adware... các phần mềm bảo mật không thể nào kiểm soát tốt được.Kẻ thù dấu mặt: Các trình duyệtMột nguyên nhân mà máy tính dễ bị tấn công và sự xâm nhập tràn lan của các sâu và virus là do những lỗ hổng trong trình duyệt. Hầu hết các phần mềm gián điệp và virus xâm nhập vào máy tính qua trình duyệt Web. Theo báo cáo của Symantec, có khoảng 70% đến 80% lây nhiễm qua trình duyệt bằng cách sử dụng ActiveX. Các điều khiển ActiveX cho phép tải và cài đặt các tiện ích cắm thêm vào trình duyệt đơn giản, nhanh chóng nhưng đó cũng là yếu điểm lớn nhất của IE về bảo mật.
Trong khi những vấn đề gây tranh cãi xung quanh các phần mềm bảo mật, thì cách tốt nhất bạn hãy tự bảo vệ mình. Nếu sử dụng IE là trình duyệt mặc định, hãy đọc bài viết Thủ thuật giúp Internet Explorer bảo mật hơn để an toàn hơn. Nếu thực sự "nhàm chán" với IE, hãy chuyển qua sử dụng Firefox hoặc Opera cũng là sự lựa chọn đáng cân nhắc.
Tuy nhiên, chẳng có trình duyệt nào là hoàn hảo và tuyệt đối an toàn. Một cách tự bảo vệ khá hữu hiệu là chuyển qua sử dụng một tài khoản không có quyền quản trị hệ thống (non-administrator)

trong HĐH Windows XP cũng là một cách tốt để hạn chế rủi ro khi lướt Web.
Minh Phúc