Supercookies, Zombie Cookies và Evercookies là gì và có gây hại không?

Việc bị theo dõi luôn là một trong những vấn đề về bảo mật riêng tư lớn nhất đối với những người sử dụng cookie, nhưng điều đó đã thay đổi nhờ Internet. Mặc dù trình duyệt cookie thông thường tỏ ra khá là hữu ích và dễ dàng dọn dẹp, nhưng có các biến thể khác được xây dựng để gắn bó và theo dõi các hoạt động duyệt web của người dùng. Hai trong số các biến thể này là supercookies và zombie cookies (thường được biết đến với cái tên "Evercookies"). Hai biến thể này nổi tiếng bởi chúng gây ra rất nhiều khó khăn cho những người muốn gỡ bỏ chúng. May mắn thay, chúng đã “nhận” được những sự quan tâm thích đáng của các nhà bảo mật, và các trình duyệt web hiện nay đang không ngừng phát triển để chống lại những kỹ thuật theo dõi lén lút phức tạp này.

Supercookies

Thuật ngữ này có thể hơi khó hiểu vì nó được sử dụng cùng lúc để mô tả một số công nghệ khác nhau, trong khi chỉ một vài trong số đó thực sự là cookie. Nói chung, thuật ngữ này đề cập đến những thứ có thể làm thay hồ sơ duyệt web của bạn để cung cấp cho bạn một ID duy nhất. Bằng cách này, chúng hỗ trợ những chức năng tương tự như cookie, cho phép các trang web và nhà quảng cáo theo dõi bạn, nhưng không giống như cookie, chúng không thể bị xóa.

Bạn sẽ thường nghe đến thuật ngữ “supercookie” được sử dụng trong tham chiếu đến Unique Identifier Headers (UIDH) và là lỗ hổng trong HTTP Strict Transport Security (HSTS), mặc dù cụm từ gốc đề cập đến các cookie bắt nguồn từ các tên miền cấp cao nhất. Điều này có nghĩa là cookie có thể được đặt cho tên miền như “.com” hoặc “.co.uk”, cho phép bất kỳ trang web nào có hậu tố tên miền đó đều có thể nhìn thấy nó.

Nếu Google.com thiết lập một supercookie, cookie đó sẽ có thể hiển thị cho bất kỳ trang web ".com" nào khác. Đây rõ ràng là một vấn đề về riêng tư, nhưng vì nó mặt khác lại là một cookie thông thường nên hầu hết các trình duyệt hiện đại đều chặn chúng theo mặc định. Bởi vì không ai nói nhiều về loại supercookie này nữa nên bạn sẽ thường nghe nhiều về hai loại kia (Zombie Cookies và Evercookies) hơn.

Unique Identifier Header (UIDH)

Một Unique Identifier Header (tiêu đề định danh duy nhất) thường không có trên máy tính của bạn, nó xuất hiện giữa ISP của bạn và máy chủ của trang web. Dưới đây là cách thức UIDH được tạo ra:

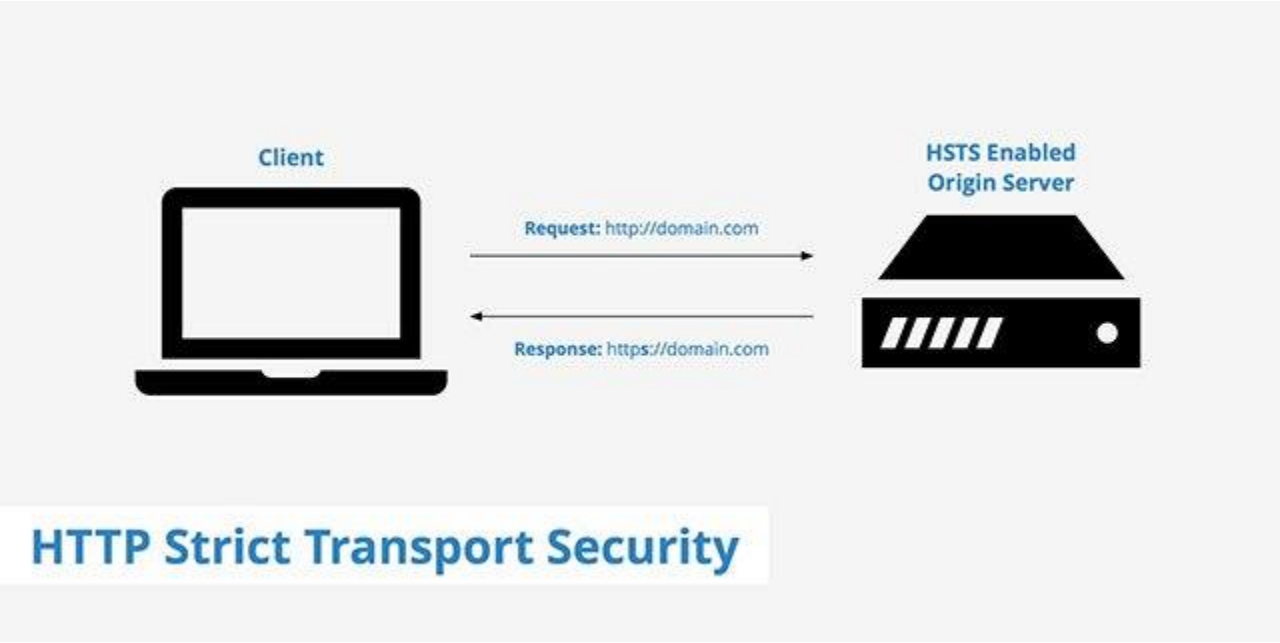
1. Bạn gửi yêu cầu về một trang web đến ISP của bạn.
2. Trước khi ISP của bạn chuyển tiếp yêu cầu tới máy chủ, nó sẽ thêm một chuỗi định danh duy nhất vào tiêu đề của yêu cầu của bạn.

3. Chuỗi định danh duy nhất này cho phép các trang web xác định bạn là cùng một người dùng bất cứ khi nào bạn truy cập, ngay cả khi bạn đã xóa cookie của chúng. Khi các trang web biết bạn là ai, chúng chỉ cần thiết lập cùng một cookie thẳng vào trình duyệt của bạn.

Nói một cách đơn giản, nếu ISP đang sử dụng theo dõi UIDH, nó sẽ gửi "chữ ký" cá nhân của bạn tới mọi trang web mà bạn truy cập. Điều này chủ yếu hữu ích trong việc tối ưu hóa doanh thu quảng cáo, nhưng nó đủ gây khó chịu đến mức FCC đã phạt Verizon 1,35 triệu USD vì không thông báo cho khách hàng của họ về việc đó, hoặc không cung cấp cho họ tùy chọn không tham gia.

Ngoài Verizon, không có nhiều dữ liệu mà ở đó các công ty đang sử dụng thông tin kiểu UIDH, nhưng phản ứng dữ dội của người tiêu dùng đã khiến nó trở thành một chiến lược không được ưa chuộng và phổ biến cho lắm. Thậm chí nó chỉ hoạt động trên các kết nối HTTP không được mã hóa. Ngoài ra,vì hầu hết các trang web hiện nay đều sử dụng HTTPS theo mặc định và bạn có thể dễ dàng tải xuống các tiện ích như HTTPS Everywhere, supercookie này thực sự không còn là vấn đề lớn nữa và có thể sẽ không được sử dụng rộng rãi. Nếu bạn muốn tăng cường thêm các lớp bảo vệ, hãy sử dụng VPN. VPN đảm bảo rằng yêu cầu của bạn sẽ được chuyển tiếp đến trang web mà không cần đính kèm UIDH.

HTTPS Strict Transfer Security (HSTS)



HSTS (HTTP Strict Transport Security) là một chính sách bảo mật cần thiết để bảo vệ các trang web bảo mật HTTPS chống lại các cuộc tấn công cấp thấp. HSTS đảm bảo rằng tất cả kết nối tới một website phải được mã hóa bằng giao thức HTTPS, và không bao giờ sử dụng giao thức HTTP. Hiện nay Google đang áp dụng HSTS cho 45 tên miền cao cấp nhất, bao gồm các tên miền có đuôi .google, .how và .soy.

HSTS thực sự là một giải pháp tốt. Nó cho phép trình duyệt của bạn chuyển hướng an toàn tới phiên bản HTTPS của trang web thay vì phiên bản HTTP không an toàn. Thật không may, nó cũng có thể được sử dụng để tạo ra một supercookie với công thức như sau:

1. Tạo nhiều tên miền phụ (như “domain.com,” “subdomain2.domain.com”...).
2. Chỉ định cho mỗi khách truy cập vào trang chính của bạn một số ngẫu nhiên.
3. Buộc người dùng tải tất cả tên miền phụ của bạn bằng cách thêm chúng vào các pixel ẩn trên một trang hoặc chuyển hướng người dùng qua từng tên miền phụ trong khi tải trang.
4. Đối với một số tên miền phụ, chúng yêu cầu trình duyệt của người dùng sử dụng HSTS để chuyển sang phiên bản bảo mật. Đối với một số loại khác, chúng để lại tên miền dưới dạng HTTP không an toàn.
5. Nếu chính sách HSTS của tên miền phụ được bật, nó được tính là “1.” Nếu nó tắt, nó được tính là “0”. Sử dụng chiến lược này, trang web có thể ghi số ID ngẫu nhiên của người dùng dưới dạng nhị phân trong cài đặt HSTS của trình duyệt.
6. Mỗi khi khách truy cập quay trở lại, trang web sẽ kiểm tra các chính sách HSTS trên trình duyệt của người dùng, HSTS sẽ trả về cùng một số nhị phân ban đầu được tạo giúp xác định người dùng.

Nghe có vẻ phức tạp, nhưng tóm lại là trang web có thể khiến trình duyệt của bạn tạo và nhớ cài đặt bảo mật cho nhiều trang và lần tiếp theo bạn truy cập, nó có thể cho biết bạn là ai thông qua những dữ liệu thu được.

Apple cũng đã đưa ra các giải pháp cho vấn đề này, ví dụ như chỉ cho phép cài đặt HSTS được đặt cho một hoặc hai tên miền chính trên mỗi trang web và hạn chế số lượt chuyển hướng mà các trang web được phép sử dụng. Các trình duyệt khác

cũng có khả năng tuân theo các biện pháp bảo mật này (chế độ ẩn danh của Firefox là một ví dụ), nhưng vì không có bất kỳ xác nhận nào được đưa ra về tính hiệu quả nên đây không phải là ưu tiên hàng đầu đối với hầu hết các trình duyệt. Bạn có thể tự mình giải quyết các vấn đề bằng cách tìm hiểu thêm về một số cách cài đặt và xóa các chính sách HSTS theo cách thủ công.

Zombie cookies/Evercookies

Zombie cookies, hay còn được gọi là Evercookie thực chất là một API JavaScript được tạo ra để minh họa những khó khăn mà bạn sẽ phải đối mặt trong nỗ lực xóa một cookie.

Zombie cookies không thể bị xóa vì chúng được ẩn bên ngoài bộ nhớ cookie thông thường của bạn. Bộ nhớ lưu trữ cục bộ là một mục tiêu chính của các Zombie cookies (Adobe Flash và Microsoft Silverlight sử dụng điều này rất nhiều) và một số lưu trữ HTML5 cũng có thể là một vấn đề. Các Zombie cookie thậm chí có thể nằm ngay trong lịch sử duyệt web của bạn hoặc trong các mã màu RGB mà trình duyệt của bạn cho phép lưu vào bộ nhớ cache.

Tuy nhiên, nhiều lỗ hổng bảo mật đang dần biến mất. Flash và Silverlight không phải là một phần quan trọng trong thiết kế web hiện đại và nhiều trình duyệt hiện nay không dễ bị tổn thương bởi Evercookie nữa. Vì có rất nhiều cách khác nhau mà các cookie này có thể chen lấn và "ký sinh" trong hệ thống của bạn, sẽ không có cách nào để tự bảo vệ mình, Tuy nhiên thói quen dọn dẹp trình duyệt không bao giờ là một biện pháp tồi.

Chung ta có đang được an toàn hay không?

Phát triển công nghệ theo dõi trực tuyến là một cuộc đua không không ngừng nghỉ trong thế giới bảo mật ngày nay, vì vậy nếu tính riêng tư là điều mà bạn đặc biệt quan tâm, bạn có lẽ nên quen với thực tế rằng chúng ta không bao giờ được bảo đảm an toàn 100% trong môi trường trực tuyến.

Tuy nhiên bạn cũng không cần phải lo lắng quá nhiều về những supercookies vì chúng không xuất hiện quá phổ biến và đang ngày càng bị ngăn chặn quyết liệt hơn. Các cookie này vẫn có khả năng hoạt động cho đến khi mọi lỗ hổng được vá, đồng thời chúng luôn có thể được cập nhật các kỹ thuật mới.