BÀN PHÍM CŨNG TIỀM TÀNG HIỂM HOẠ BẢO MẬT

Các nhà khoa học vừa cảnh báo các thiết bị ngoại vi như bàn phím, chuột hoặc tai nghe cũng là một hiểm hoạ bảo mật đối với máy tính. Bản thân những thiết bị ngoại vi đó đã mắc lỗi và chúng hoàn toàn có thể bị lợi dụng để ăn cắp dữ l

Các nhà khoa học vừa cảnh báo các thiết bị ngoại vi như bàn phím, chuột hoặc tai nghe cũng là một hiểm hoạ bảo mật đối với máy tính. Bản thân những thiết bị ngoại vi đó đã mắc lỗi và chúng hoàn toàn có thể bị lợi dụng để ăn cắp dữ liệu. Các chuyên gia nghiên cứu đến từ Trường khoa học kỹ thuật ứng dụng thuộc Trường ĐH Pennsylvania đặt tên những phần cứng bị lỗi là JitterBugs. Cái tên JitterBugs đã có lên cách những thiết bị ngoại vi đó gửi đi rất nhiều các loại dữ liệu ăn cắp được nhờ vào việc chèn thêm các khoảng trễ không thể nhận thấy được trong quá trình xử lý mỗi khi có một phím trên bàn phím được nhấn. JitterBug là gì? Về mặt khái niệm, các thiết bị JitterBugs cũng tương tự như các chương trình độc hại keylogger chuyên thu thập dữ liệu bằng cách ghi nhận các thao tác bàn phím. Điểm khác biệt là thiết bị JitterBugs cần phải được gắn trực tiếp vào hệ thống PC trong khi đó keylogger lại có thể tự động cài đặt. Để minh chứng cho cảnh báo của mình các nhà nghiên cứu thuộc Khoa khoa học máy tính và thông tin của Trường ĐH Pennsylvania cùng với một sinh viên sau đại học Gaurav Shah và giáo sư Matthew Blaze đã phát triển thành công một chiếc bàn phím JitterBug một cách khá dễ dàng. Các thiết bị JitterBugs cũng có thể thu thập thông tin từ bất kỳ một phần mềm ứng dụng tương tác nào cần có sự kết hợp giữa các hoạt động của bàn phím và hoạt động của hệ thống mạng. Lấy ví dụ như các ứng dụng tin nhắn tức thời, SSH hoặc ứng dụng điều khiển PC từ xa. JitterBugs lấy dữ liệu bằng cách chèn thêm các khoảng trễ rất khó có thể phát hiện vào quá trình xử lý dữ liệu mỗi khi người dùng nhấn một phím trên bàn phím. "Đây có thể xem là một hình thức gián điệp. Một người nào đó chỉ cần tiếp cận trực tiếp với máy tính của bạn và cài đặt một thiết bị JitterBug. Không những thế việc che dấu các thiết bị JitterBug cũng rất dễ dàng hoặc thậm trí là cung cấp cho người dùng một chiếc bàn phím JitterBug," Shah nói. Tiềm tàng những mối nguy Trong một kịch bản mà giáo sư Blaze gọi là "Supply Chain Attack", các nhà sản xuất thiết bị ngoại vi sẽ bị tấn công và dẫn đến hậu quả là sẽ có rất nhiều bàn phím mắc lỗi JitterBug được tung ra thị trường. Kẻ tấn công chỉ cần đợi cho đến khi nào những chiếc bàn phím đó được lắp đặt và nhận dữ liệu về. Shah cho biết kênh mà JitterBug sử dụng để gửi dữ liệu đi cũng chính là điểm yếu nhất của lỗi này. Điểm yếu này có thể sử dụng để phát hiện và đối phó với JitterBug. Và mặc dù mới chỉ trình bày những giải pháp đối phó đơn giản với JitterBug nhưng những kết quả ban đầu của Shah cho thấy sử dụng kỹ thuật mật mã để che dấu các kênh Jitter đã được mã hoá sẽ là một giải pháp đầy tính hứa hẹn. Chưa từng được nghĩ tới "Chúng ta thường nghĩ rằng bàn phím hay những thiết bị đầu vào là hoàn toàn an toàn. Tuy nhiên nghiên cứu của chúng tôi đã cho thấy nếu chúng ta muốn một hệ thống thật an toàn thì chúng ta cũng phải bảo đảm những thiết bị nói trên cũng an toàn," Shah khẳng định. "Mặc dù chúng tôi chưa có bất kỳ một bằng chứng nào về việc đã có một ai đó sử dụng JitterBug, nhưng điều mà chúng tôi muốn nói lên đằng sau cảnh báo đó là nếu chúng tôi đã có thể sản xuất được thiết bị JitterBug thì chắc chắn sẽ có người làm được," Shah khẳng định. "Không ngoại trừ đó là kẻ xấu." Hoàng Dũng