LAPTOP CÓ THỂ BỊ KHỐNG CHẾ QUA TRÌNH ĐIỀU KHIỂN WI-FI

Các chuyên gia nghiên cứu bảo mật vừa khám phá ra một thủ thuật mới, cho phép họ kiểm soát toàn bộ hệ thống máy tính xách tay bằng cách cài một mã lỗi vào trình điều khiển (driver) thiết bị kết nối Internet không dây phạm vi hẹp

Các chuyên gia nghiên cứu bảo mật vừa khám phá ra một thủ thuật mới, cho phép họ kiểm soát toàn bộ hệ thống máy tính xách tay bằng cách cài một mã lỗi vào trình điều khiển (driver) thiết bị kết nối Internet không dây phạm vi hẹp. Chi tiết quá trình tấn công sẽ được chuyên gia phân tích David Maynor của công ty bảo mật Internet ISS mô tả tại Diễn đàn Black Hat 2006, diễn ra trong tháng tới ở Las Vegas,Mỹ. Khai thác trình điều khiển thiết bị là một nhiệm vụ không hề dễ dàng, nhưng thời gian gần đây nó đã trở nên khả thi hơn nhờ sự xuất hiện của một số công cụ phần mềm mới, hỗ trợ cả những hacker không thực sự am hiểu về kỹ thuật (còn được gọi là script kiddie - người không biết nhiều về công nghệ nhưng vô tình có được thông tin về điểm yếu của thiết bị qua Internet và giành quyền quản lý hệ thống). Chuyên gia Maynor đã thử dùng công cụ tấn công 802.11 nguồn mở mang tên LORCON nhằm phát tán một lượng lớn các gói dữ liệu không dây tới nhiều thẻ wireless khác nhau. Hacker thường sử dụng phương pháp này để kiểm tra xem chương trình chỉ bị trục trặc hay có thể tạo cơ hội cho họ xử lý phần mềm nguy hiểm trên laptop của nạn nhân. Nhờ LORCON, Maynor còn tìm thấy một lỗi driver cho phép ông kiểm soát toàn bộ hệ thống. Mayor cũng đang lặp lại thí nghiệm này trên các công nghệ mạng khác như Bluetooth, EvDO và HSDPA. "Hacker chỉ cần ngồi tại một điểm kết nối công cộng và ung dung đợi 'con mồi' xuất hiện trong tầm ngắm", Mayor cảnh báo. "Hệ thống của người sử dụng sẽ bị tấn công ngay cả khi driver mới được bật lên và chưa hoàn thành quá trình kết nối mạng". Theo Mayor, nguyên nhân chính của tình trạng này là các chuyên gia soạn trình điều khiển cho thiết bị không dây hiện nay không mảy may nghĩ đến vấn đề bảo mật.