PASSWORD CÀNG ĐƠN GIẢN CÀNG DỄ BỊ HACK

Một ng

Một nghiên cứu mới đây cho biết, bốn máy tính Linux thử nghiệm cài mật khẩu đơn giản phải "đối đầu" với 270.000 đợt tấn công với mật độ cứ 39 giây có 1 đợt tấn công, trong suốt 42 ngày liền.

Những hệ thống mã mở này được một nhà nghiên cứu tại ĐH Maryland (Mỹ) cố tình bỏ ngỏ nhằm tìm hiểu xem những hacker tấn công các máy tính này ra sao?

Trong số những kết quả thu được, các nhà nghiên cứu đã nhận thấy: mật khẩu đơn giản "gián tiếp" giúp công việc của các hacker trở nên thuận lợi hơn. Nghiên cứu này cũng chỉ ra rằng sự lựa chọn sử dụng tên đăng nhập cùng với những mật khẩu kèm theo một cách cẩn thận có thể tạo ra sự khác biệt lớn trong chuyện liệu những hacker có đột nhập vào máy tính của người nào đó hay ko?

Nhiều người dùng máy tính đặt mật khẩu theo kiểu "dễ nhớ", "dễ thuộc" mà quên mất đòi hỏi bảo mật cao

Nghiên cứu này do Michel Cukier, một giáo viên trợ giảng của khoa kỹ thuật máy tính dẫn dắt. Mục đích của Cukier là tìm hiểu xem các hacker hành động thế nào khi tấn công hệ thống máy tính - và những bước tiếp theo của họ một khi đã xâm nhập vào hệ thống này.

Sử dụng những công cụ phần mềm giúp hacker có thể đoán biết tên đăng nhập và mật khẩu, nghiên cứu này đã ghi nhận những từ khóa phổ biến nhất mà hacker thường sử dụng với nỗ lực đăng nhập được hệ thống. Cukier cùng hai sinh viên của mình đã phát hiện rằng hầu hết những cuộc tấn công do hacker tiến hành đều thông qua phương thức sử dụng những tập lệnh từ điển

chạy qua danh sách các đăng nhập và mật khẩu thông thường nhằm phá vỡ "rào cản đầu tiên" của máy tính.

Trong toàn bộ các cuộc tấn công, có tới 825 cuộc thành công về cơ bản và các hackers có thể kiểm soát hoàn toàn hệ thống. Cuộc nghiên cứu đã được tiến hành từ 14/11 đến 8/12/2006.

Cukier không hề bất ngờ trước kết quả thu được. Trong những đợt tấn công này, "root" là từ khóa dự đoán hàng đầu của những tập lệnh từ điển, chiếm tới 12,34%, trong khi đó từ "admin" là 1,63%. Từ "test" chiếm 0,84%, "guest" chiếm 0,84%.

Phần mềm tập lệnh từ điển đã thử sử dụng mật khẩu trùng với tên đăng nhập tới 43% thời gian để mở đường vào hệ thống, Cukier cho biết. Nguyên nhân, theo ông, là bởi hacker luôn cố gắng cho những sự kết hợp đơn giản nhất bởi chúng thực sự thường trùng khớp với nhau.

Một khi đã ở trong hệ thống, những hacker đã kiểm soát được nhiều chức năng cơ bản, bao gồm kiểm tra cấu hình phần mềm, thay đổi mật khẩu, kiểm tra ổ cứng và/ hoặc cấu hình phần mềm lần nữa, tải một file, cài đặt các chương trình trợ tải và sau đó chạy chương trình.

Đối với những nhân viên bảo mật CNTT, cuộc nghiên cứu này đã càng củng cố nhận định: "Mật khẩu đơn giản đang là một vấn đề đau đầu", Cukier nhận định.

Tại ĐH Maryland, người dùng đã được lưu ý nên đặt những mật khẩu gồm ít nhất 8 ký tự, với ít nhất một ký tự viết hoa và một ký tự viết thường, đồng thời khuyên rằng ít nhất có một ký tự là chữ số hoặc biểu tượng dấu chấm. Tất cả những mật khẩu nên cứ 180 ngày được thay đổi 1 lần..

"Biện pháp này thực sự là hợp lý", Cukier nói. "Nó sẽ không hữu ích đối với những mật khẩu quá phức tạp khiến mọi người không thể nhớ nổi và (theo đó) sẽ viết xuống một tờ giấy ghi nhớ dán trước màn hình máy tính".

Người dùng có thể sử dụng tựa đề của một quyển sách yêu thích để đặt mật khẩu hoặc thậm chí những ký tự đầu tiên của một câu nói bất hủ nào đó, ông cho biết. "Với những mật khẩu này bạn có thể nhớ một cách dễ dàng mà không phải viết nó ra giấy".

Anh Thư