ZONEALARM VẪN CÓ THỂ BỊ "LỪA"

<input type="image" height="150" hspace="2"

Các chuyên gia bảo mật vừa mới cảnh báo về một loại mã nguy hiểm mới có thể giả dạng các ứng dụng để lừa tường lửa ZoneAlarm cho phép chúng được kết nối với Internet mở cổng cho tin tặc tấn công.Tuy nhiên, Zone Labs – nhà phát triển ứng dụng tường lửa cá nhân ZoneAlarm – trong bản tin khuyến cáo bảo mật công bố ngày 01/09 cho biết phương thức tấn công hoàn toàn mới này chỉ có thể qua mặt được phiên bản ZoneAlarm miễn phí hoặc các phiên bản thương mại từ 5.5 trở về trước và Check Point Integrity Client được cài đặt và sử dụng ở chế độ mặc định. Các phiên bản từ 6.0 trở lên không mắc lỗi này.Nếu thành công trong việc lừa ứng dụng tường lửa, các đoạn mã chương trình nguy hiểm như thế này sẽ giành được quyền kết nối vào Internet nhưng phải thông qua một ứng dụng khác. Còn nếu những đoạn mã chương trình này yêu cầu kết nối Internet trực tiếp thì vẫn bị ZoneAlarm chặn lại.Đầu tuần qua chuyên gia nghiên cứu bảo mật Debasis Mohanty đã cho công bố một ví dụ về việc ứng dụng phương thức tấn công này. Theo đó tin tặc có thể lợi dụng một cơ chế của hệ điều hành Windows để liên kết các ứng dụng khác nhau – như tin tặc có thể liên kết một chương trình keylogger với Internet Explorer chẳng hạn nhằm cho phép chương trình nguy hiểm chuyên dùng ăn cắp thông tin cá nhân được phép kết nối và gửi thông tin về cho tin tặc.Bên cạnh đó, Mohanty cũng cảnh báo lỗi này có thể cũng có trong các ứng dụng tường lửa khác không riêng gì ZoneAlarm.Tuy nhiên, John LaCour, giám đốc phụ trách dịch vụ bảo mật của Zone Labs, cho biết cho đến nay hãng chưa phát hiện ra được bất kỳ một chương trình nguy hiểm nào sử dụng phương thức này để qua mặt ZoneAlarm. "Đây chỉ là một phương thức tấn công trên lý thuyết và chúng sẽ không bao giờ được ứng dụng vào thực tế". Zone Labs xếp lỗi này vào mức độ không nguy hiểm.Zone Labs hiện vẫn chưa có kế hoạch sửa lỗi bảo mật mới này cho các phiên bản tường lửa miễn phí. Người sử dụng các phiên bản thương mại ZoneAlarm 5.5, Check Point Integrity Client phiên bản 6.0 và 5.5 có thể tự bảo vệ mình khỏi lỗ hổng bảo mật này bằng cách kích hoạt tính năng Advanced Program Control hoặc nâng cấp lên phiên bản mới hơn.HVD - (ZDNet)