

TIN TẶC VÔ HIỆU HOÁ WINDOWS FIREWALL

Hacker

Hacker vừa tung lên mạng một đoạn mã độc hại có khả năng vô hiệu hoá hoàn toàn Windows Firewall trên một số PC chạy Windows XP.

Cụ thể đó là những PC chạy Windows XP và có kích hoạt dịch vụ hệ thống Internet Connection Service (ICS). Đây là dịch vụ hệ thống cho phép người dùng Windows có thể biến chiếc PC của họ thành một chiếc router và chia sẻ kết nối Internet với các PC khác trong cùng một mạng LAN.

Kẻ tấn công có thể gửi những gói dữ liệu “độc” tới một PC Windows XP có kích hoạt ICS để vô hiệu hoá dịch vụ hệ thống này. Tuy nhiên, ICS lại có liên hệ trực tiếp với Windows Firewall, chính vì thế nếu ICS ngừng hoạt động thì Windows Firewall cũng “chết” theo.

Tyler Reguly – chuyên gia nghiên cứu của hãng bảo mật nCircle Network Security – là người đã phát hiện ra đoạn mã này và công bố trên trang blog của ông.

Nguy cơ?

Reguly khẳng định không chỉ có Windows XP có thể bị tấn công bằng đoạn mã “độc” trên mà cả Windows Server 2003.

Tuy nhiên, những điều tra ban đầu của Microsoft khẳng định mới chỉ có Windows XP là có thể bị tấn công bằng mã “độc” vừa được phát hiện. Hiện Microsoft vẫn chưa phát hiện được bất kỳ một vụ tấn công nào thông qua việc lợi dụng đoạn mã độc này.

Vô hiệu hoá được Windows Firewall, bọn tin tặc sẽ có thêm nhiều phương thức tấn công người dùng. Tuy nhiên, có vẻ như những phương thức tấn công chưa đạt được nhiều hiệu quả lắm, Reguly khẳng định.

Lấy ví dụ, để có thể tấn công được người dùng thì kẻ tấn công phải là một thành viên của mạng LAN và đó phải là mạng LAN có sử dụng dịch vụ hệ thống ICS. Một yếu tố nữa là phương thức tấn công theo kiểu này hoàn toàn bất lực trước các hệ thống tường lửa của hãng thứ ba khác.

Người dùng hoàn toàn có thể tránh nguy cơ bị tấn công bằng cách vô hiệu hoá dịch vụ hệ thống ICS. Nhưng nếu vô hiệu hoá dịch vụ ứng dụng này thì lại đồng nghĩa với việc không thể chia sẻ

kết nối Internet.

Giải pháp

Giải pháp đơn giản nhất là thay vì sử dụng dịch vụ hệ thống ICS người dùng nên sử dụng một router chuyên biệt hoặc thiết bị NAT (Network Address Translation), Stefano Zanero – Giám đốc kỹ thuật của Secure Network SRL – cho biết.

“Phần lớn những thiết bị nói trên đều có giá thành khá rẻ. Không những thế một số sản phẩm còn mang đến cho người dùng nhiều giải pháp bảo vệ an toàn hơn”.

Hoàng Dũng