TƯỜNG LỬA VISTA MỚI KHÔNG CHẮC CHẮN VỚI BẢO MẬT LƯU LƯỢNG RA

Micros

Microsoft đã giới thiệu Windows Vista là một phiên bản mới cho phép có nhiều tính năng bảo mật nổi trội hơn so với Windows XP, một trong số đó làcác kỹ thuật tường lửa mới như tính năng lọc hai chiều (vào/ra).

Tuy nhiên khi được phát hành và bán rộng rãi thì người dùng bắt đầu cảm thấy tường lửa của Windows mới này cũng có rất ít tính năng bảo mật lưu lượng ra, nó không rõ nét ở chỗ làm thế nào có thể cấu hình bảo vệ lưu lượng ra để chống lại được Spyware, Trojan horse và các bot.

Các tường lửa như Windows Firewall làm việc không tích cực khi một máy tính kết nối nguy hiểm trong môi trường Internet. Tường lửa Windows XP có sự bảo vệ lượng vào nhưng lại không bảo vệ lượng ra. Nhiều malware có thể thực hiện kết nối không mong muốn hay không nhìn thấy với các hacker thông qua lượng ra và có thể trao cho chúng quyền kiểm soát PC.

Trong nhiều trường hợp, một máy tính có thể trở thành zombie hay bot, và gửi đi hàng nghìn mẩu spam thông qua kết nối lưu lượng ra mà chủ nhân máy tính không hề hay biết.

Việc cạnh trang giữa các tường lửa như ZoneAlarm, Norton Personal Firewall và McAfee Internet Security Suite cho phép người dùng cấu hình bảo vệ lưu lượng ra. Chính vì vậy khi Microsoft nghiên cứu lại về tường lửa Windows thì hãng này đã thêm vào tính năng này cho Windows Vista.

Tuy nhiên, mặc định thì tính năng lọc lưu lượng ra của tường lửa trong Windows Vista là tắt. Thêm nữa là thực tế không có cách nào có thể sử dụng bộ lọc lưu lượng ra để ngăn toàn bộ các kết nối ra không mong muốn.

Thông thường, để cấu hình tường lửa Windows Vista, bạn chọn Control Panel, sau đó Security, bật hoặc tắt Windows Firewall. Bạn sẽ nhìn thấy màn hình hiển thị như hình dưới đây.

Màn hình không cho bạn cấu hình lọc lưu lượng cho tường lửa.

Như bạn thấy, không có cách nào để cấu hình việc lọc lưu lượng ra – bạn chỉ có thể bật/tắt bộ lọc lưu lượng vào và qua các tab khác nhau bạn có thể cấu hình công việc của việc lọc vào.

Để làm việc với bộ lọc ra, bạn phải thay thế sử dụng Microsoft Management Console bằng Windows Firewall đặc biệt với Advanced Security Group Policy applet bằng việc nhập "wf.msc" vào hộp Search hoặc cửa sổ lệnh và nhấn Enter.

Hình dưới đây thể hiện điều đó.

Để cấu hình lọc lưu lượng ra, sử dụng Windows Firewall với Advanced Security Group Policy applet

Nếu bạn tìm thấy các profile khác nhau trong vùng Overview thì sẽ thấy với mỗi profile sẽ là "Các kết nối lưu lượng ra không hợp lệ với phương thức được cho phép"

Mỗi phương thức trong Windows Firewall cung cấp các kết nối lưu lượng ra. Kích vào biểu tượng Outbound Rules ở bên trái của màn hình thì bạn sẽ thấy tất cả các phương thức lưu lượng ra. Với hình dưới đây, mỗi một phương thức cho phép các kết nối lưu lượng ra. Không khóa kết nối.

Mỗi một phương thức cho phép các kết nối lưu lượng ra

Để ngăn chặn được malware tạo các kết nối ra, bạn phải biết tất cả những chi tiết về hàng nghìn malware đang sống sót, và tạo ra các phương thức cho mỗi một loại riêng biệt. Đó quả thực là điều không tưởng vì bạn không thể biết được hết về malware mà chúng chưa được phát hiện.

Việc cạnh tranh giữa các tường lửa thường cho phép những chương trình cụ thể thực hiện kết nối ra và thông báo khi chương trình khác thực hiện kết nối. Bạn có thể gọi tên chương trình, thực thi và đưa ra quyết định các trường hợp mà chương trình được phép. Sau đó có thể khóa hoặc cho phép chương trình thực hiện kết nối trong một thời điểm nào đó hoặc thường xuyên.

Phản ứng từ phía Microsoft

Microsoft lại khẳng đinh rằng tường lửa có thể thực hiện được việc lọc lưu lượng ra nhưng những gì mà nó thực hiện thì người dùng không hề nhìn thấy được. Jason Leznek, giám đốc sản phẩm của Microsoft đã nói rằng các phương thức lọc lưu lượng ra "đã được kích hoạt mặc định trong các dịch vụ bên trong của Windows như một phần của Windows Service Hardening, điều đó cho phép tường lửa hiểu các dịch vụ cụ thể của Windows và khóa nếu chúng thực hiện một vấn đề gì đó không được mong đợi từ trước, ví dụ như thông qua một lỗ hổng đã bị khai thác. Windows Firewall cũng bảo vệ các máy tính bằng việc khóa các tin nhắn ra cụ thể để bảo đảm máy tính chống lại được việc các kẻ tấn công có thể thực hiện quét các cổng."

Theo cách khác, Microsoft cũng khẳng định rằng tường lửa có thể khóa nhiều malware. Nhưng Leznek thừa nhận rằng nó không thể khóa tất cả malware và ông ấy cũng khẳng định rằng phương pháp hiệu quả hơn đối với việc lọc lưu lượng ra là sử dụng công cụ chống Spyware như Windows Defender, mô đun này đã được công ty khẳng định sẽ không cho phép malware có thể cài đặt lên máy tính của bạn.

Điều này lại trái ngược với những gì mà giám đốc sản phẩm của nhóm Vista Greg Sullivan đã nói với BusinessWeek. "Việc lọc lưu lượng ra là một giải pháp tốn kém với những gì mà chúng ta không thấy có nhiều lợi ích", ông ta cũng nói thêm với tạp chí này: "Nó sẽ là gánh nặng cho tất cả chúng tôi, các đối tác của chúng tôi và hầu hết các nhà sản xuất vì giá thành cao mà chỉ thu lại được ít lợi ích từ đó"

Tuy nhiên Microsoft cũng có một số phương pháp để bảo vệ lưu lượng ra. Khi được hỏi về những cần thiết cho việc lọc này, Leznek đã nói rằng Windows Live OneCare, một sản phẩm và dịch vụ có thu phí mà Microsoft bán khoảng 49.95$ hàng năm, "cung cấp việc lọc lưu lượng ra như một dịch vụ và có thể là một tùy chọn hấp dẫn".

Chính vì vậy nên thậm chí việc lọc hai chiều không thể sử dụng mở rộng trong Windows Firewall thì bạn cũng hoàn toàn có thể mua các gói phần mềm mở rộng của Microsoft.

Vậy thì kết luận ở đây là gì? Nếu bạn là một người dùng Windows Vista và muốn bảo đảm có cấu hình lọc lưu lượng hai chiều thì bạn cần phải mua cả OneCare Live, các sản phẩm bảo mật khác hoặc tường lửa để cung cấp bảo vệ lưu lượng ra cũng như lưu lượng vào. Bạn cũng phải cẩn thận một điều là không phải tất cả phần mềm nào cũng hoạt tốt trên Windows Vista.