BẢO MẬT VISTA

Cho dù Windows Vista có lẽ an toàn hơn Windows XP nhưng hệ điều hành mới này của Microsoft đã cho thấy dễ bị tấn công.

Cuối tháng 3 vừa qua, trong khi các nhà nghiên cứu bảo mật đang "bù đầu bù cổ" với các kiểu tấn công dạng download thì họ phát hiện điều bất ngờ: có một lỗ hổng khác nằm ở cách Windows xử lý tập tin con trỏ động (.ani), không loại trừ Windows XP. Lỗ hổng này cũng ảnh hưởng đến Vista, hệ điều hành được Microsoft chú trọng nhiều về bảo mật.

Các chuyên gia bảo mật vẫn cho rằng Vista tiến bộ hơn nhiều so với các phiên bản Windows trước. Theo họ, Vista đã thêm những tính năng bảo mật mới, trong đó có tường lửa cải tiến, chế độ "Protected Mode" cho Internet Explorer và User Account Control. Những tính năng này giúp Vista chống chọi tốt hơn trước các loại tấn công phổ biến của phần mềm gián điệp và phần mềm ác ý. Nhưng lỗ hổng nêu trên (đã được sửa) là "vết bùn" của Microsoft để lại, cộng thêm 2 bản vá bảo mật quan trọng khác được tung ra cho Vista trong 3 tháng đầu tiên ra mắt. Chuyện này ít nhiều ảnh hưởng đến tiếng thơm về bảo mật của Vista (xem thêm mục "Các lỗ hổng của Vista"). Vista có thể an toàn hơn nhưng người dùng vẫn phải bận tâm đến bảo mật.

Áo chống đạn còn mỏng

User Account Control (UAC) là công cụ tốt nhất trong nhóm này. Theo dự đoán của chính Microsoft, có đến 95% người dùng hệ điều hành Windows trước khi Vista xuất hiện, thường chạy các ứng dụng quen thuộc với tài khoản quản trị, mà với tài khoản này họ có quyền chỉnh sửa hệ thống. Nhưng điều này cũng tiếp tay cho tin tặc tấn công PC dễ dàng. Mặc định, UAC yêu cầu mật khẩu cho mỗi tác vụ, tránh cho người dùng, hoặc các chương trình ác ý, không thể thay đổi hay can thiệp vào được những vùng nhạy cảm của hệ điều hành.

Ứng dụng chống phần mềm gián điệp tích hợp của Vista – Windows Defender – cho bạn quét hàng ngày, nhưng khi thử nghiệm, công cụ lại bỏ sót khoảng 1/3 tổng số mẫu phần mềm gián điệp và phần mềm quảng cáo.

Nhưng chính bản thân UAC lại là kẻ thù lớn nhất. Các nhắc nhở dạng pop-up thường xuyên xuất hiện thực sự rất phiền phức, cụ thể là trong suốt quá trình thiết lập một hệ thống mới. Sau khoảng 10 ngày sử dụng, tần suất nhắc nhở này mới giảm đi nhưng không phải ai cũng tránh được chuyện bị nhắc nhở liên tục. Ví dụ, chỉ một điều đơn giản là bạn muốn chuyển một tập tin trong thư mục này sang thư mục khác, hệ thống cũng hiện pop-up cảnh báo.

Kết quả là nhiều người dùng Vista đã bực bội tắt UAC (vẫn có trường hợp người dùng phải bật UAC lại để có thể chạy vài game cũ yêu cầu quyền người dùng). Nhưng làm như vậy lại đụng đến chuyện bảo mật vì tắt UAC hay nhiều người bực mình cứ "cho qua" khi nhấn "Allow" vô tội vạ, làm như vậy, họ đã phớt lờ đi mục đích của UAC.

Một nhà nghiên cứu bảo mật nói rằng UAC có một điểm yếu trong thiết kế là khi cài đặt chương trình gì thì UAC đều "mở toang cửa" toàn bộ hệ thống, bất kể chương trình cài đặt đó không cần phải truy cập đến hết hệ thống (xem thêm find.pcworld.com/57069). Microsoft thừa nhận điểm yếu này nhưng điều đó lại đảm bảo an toàn cho người dùng. Hãng chưa cho biết kế hoạch có chỉnh sửa lại thiết kế của UAC hay không.

Tính năng chính thứ 2 về bảo mật của Vista chính là Windows Defender, công cụ phòng chống phần mềm gián điệp từng được hãng tung ra miễn phí cho XP và lần này được tích hợp ngay trong Vista. Mặc dù đây không phải là tiện ích chống virus đầy đủ nhưng nó có thể dễ dàng quét các phần mềm gián điệp hay phần mềm quảng cáo đang chiếm nguồn tài nguyên hệ thống. Defender cũng có "màng lọc" khi bạn tải tập tin qua Internet Explorer 7.

Đây là ý tưởng tuyệt vời. Nhưng qua thử nghiệm của AV-Test (AV-Test.org) thì Defender chỉ nhận diện được 65% trong 14.517 mẫu phần mềm quảng cáo và gián điệp trong một lần quét theo yêu cầu. So sánh với 8 công cụ chống virus khác có tích hợp chức năng chống phần mềm gián điệp thì đều có tỉ lệ nhận diện từ 73% đến 99% đối với cùng số mẫu test trên. Theo ý kiến của chuyên gia AV-Test thì Windows Defender chưa tốt. Hầu như mọi công cụ riêng lẻ hoặc công cụ tích hợp tính năng chống phần mềm gián điệp đều chứng tỏ làm tốt hơn Defender.

Tường lửa chắn tốt

Tường lửa cải tiến của Vista lại là 1 câu chuyện khác. Nó có khả năng chặn cả luồng dữ liệu đi ra và đi vào (inbound và outbound) trong khi tường lửa của XP chỉ chặn đường đi vào. Bộ lọc luồng đi ra có một lớp bảo mật thứ 2 để chặn những loại tấn công ác ý phức tạp mà chúng thường "âm thầm" móc nối hệ thống của bạn với các máy chủ do tin tặc điều khiển từ xa. Nhưng vì có nhiều dạng bảo mật ở lớp thứ 2 này nên quyết định chương trình nào được và không được phép vượt ra khỏi hệ thống lại là một vấn đề kỹ thuật khác. Vì lý do này mà Microsoft mặc định tắt luồng chặn đi ra. Thậm chí ngay cả khi không có bộ lọc luồng đi ra thì tường lửa được đánh giá là rất tốt.

Tường lửa nâng cấp của Vista có thể chặn các chương trình không tên không họ cố kết nối Internet, nhưng chức năng này theo mặc định là tắt.

Theo một chuyên gia, tường lửa của Vista luôn chạy ngầm ở nền, chặn được mọi kết nối đi vào không rõ ràng. Người dùng thông thạo có thể cấu hình bộ lọc luồng đi ra để tăng cường bảo mật; còn những ai không rành về kỹ thuật có thể không tự mình cấu hình được cho luồng ra, nhưng dù gì cũng chặn được tấn công từ ngoài vào. Mặc định, người dùng không bị ép buộc phải thiết lập bất cứ luật nào cho bộ lọc luồng đi ra.

Tường lửa Vista vượt qua được hầu hết các thử nghiệm phân tích của AV-Test. Tuy nhiên, nó không thể lọc những tập tin đính kèm trong e-mail mà một số công cụ tường lửa khác làm được. Hơn nữa, nó không phải là công cụ có tỉ lệ lọc cao nhất khi thử nghiệm với các mẫu tấn công (còn gọi là leaktest, chương trình được viết để thử nghiệm tường lửa có chặn được các ứng dụng cố "móc nối" ra Internet).

Dù vậy, nhiều công ty bảo mật và nhà nghiên cứu, trong đó có AV-Test lý luận rằng vì những mẫu chương trình thử nghiệm này là do "người trong cuộc" viết ra (khác với phần mềm ác ý) nên chúng có thể không đánh giá được chính xác khả năng của tường lửa.

Tường lửa của Vista cùng với nhiều tường lửa khác có thể làm tốt được nhiệm vụ chặn xâm nhập từ bên ngoài vào máy tính. Nhưng các chương trình Internet buộc phải đi qua tường lửa để truy cập trang web, vào hộp thư e-mail hoặc cả công cụ chat. Điều này tự nó tạo ra một kẽ hở để tin tặc tấn công.

Vì Internet Explorer mở rộng cửa vào PC của bạn và IE được rất nhiều người dùng nên trình duyệt này liên tục nằm dưới "làn đạn". Để tăng mức bảo mật cho IE7, chế độ mặc định của trình duyệt trong bản Windows Vista đều ở Protected Mode, tách biệt IE với các vùng nhạy cảm của hệ điều hành nếu lỡ IE đã bị tấn công. Chiến thuật phòng thủ này hiện đang thành công, chống được các cuộc tấn công hiện nay như là lỗi con trỏ động.

Ngoài những kiểu phòng thủ "tiền tuyến" như vậy, Vista cũng có nhiều dạng phòng ngự nền khác. Công cụ PatchGuard chặn rootkit, là chương trình dấu virus bên trong. Một kỹ thuật khác tên là Address Space Layout Randomization, khiến phần mềm ác ý khó tìm ra và lây nhiễm vào các tiến trình đang chạy. Cuối cùng, có vài thay đổi trong nhân hệ thống (kernel), là trái tim của bất kỳ hệ điều hành nào, tăng khả năng phòng chống với các kiểu tấn công của tin tặc.

Tấn công nhắm đến con người

Bạn chớ vội mừng, trong khi Vista an toàn hơn XP thì các chuyên gia đoán là kẻ xấu sẽ nhanh chóng tìm cách vượt qua được bảo mật của Vista. Một phương pháp phổ biến là sử dụng các "chiêu" tâm lý để nhắm đến con người, không phải PC. Các kỹ thuật "tâm lý" này là dạng gửi phần mềm ác ý ngụy trang trong một game hoặc một đoạn video hấp dẫn nào đó để khai thác tính tò mò hoặc không biết của người dùng, dụ họ nhấn vào một đường link hoặc một tập tin đính kèm. Nếu nhấn vào, phần mềm ác ý đã vượt qua được ½ lớp bảo mật tự động, trong đó có cả tường lửa.

Một hướng tiềm tàng khác đe doạ lớp bảo mật của Vista là tấn công vào các chương trình, không phải vào hệ điều hành. Các chương trình nghe nhìn như Adobe Flash, Apple QuickTime gần đây đã phải hứng chịu nhiều cuộc tấn công vì tin tặc phát hiện và khai thác được các điểm yếu của phần mềm, ví dụ chúng có thể tấn công qua một tập tin video trực tuyến. Để giữ cho PC an toàn, bạn nên cài bản sửa lỗi các chương trình đó, chúng cũng quan trọng như những bản sửa lỗi cho hệ điều hành. Theo một chuyên gia, bất kỳ ứng dụng nào có trên desktop đều có những lỗ hổng.

Một thông báo rõ ràng đến người dùng PC là: mặc dù kẻ xấu khó tấn công vào Vista hơn nhưng đây không phải là hệ điều hành không có kẽ hở. Bạn vẫn cần cài những bản vá để lấp những lỗ hổng được phát hiện và bạn vẫn phải dùng chương trình chống virus như đã từng dùng trong XP.

Các lỗ hổng của Vista

• Con trỏ động: một lỗi trong mã con trỏ động có trong hệ điều hành từ Windows 2000 SP4 đến Vista. Với các tập tin .ani, .cur hoặc .ico, kẻ tấn công từ xa có thể tạo lỗi tràn bộ đệm, "tống" nhiều dữ liệu vào một chương trình để chương trình đó bị quá tải. Điều này cho phép kẻ xấu xâm nhập PC của người dùng. Microsoft đã sửa lỗi này với bản vá MS07-017.

• Malware Protection Engine: một lỗ hổng chí mạng trong mọi phiên bản Windows sử dụng Microsoft Malware Protection Engine, được áp dụng trong công cụ chống phần mềm gián điệp Windows Defender và phần mềm công cụ quét virus OneCare của Microsoft. Lỗi này có thể ép hệ thống chạy các đoạn mã tấn công khi nó quét một tập tin PDF đã bị nhiễm. Bạn có thể sửa lỗi này với bản vá MS07-010.

• CSRSS: một lỗ hổng trong cách xử lý lỗi của Windows Client/Server Runtime Server Subsystem (CSRSS) có thể cho phép kẻ tấn công "xóa sổ" tính năng UAC (User Account Control) của Vista. Sửa lỗi này bằng bản vá MS07-021.