LÁCH QUA BẢO MẬT VISTA

Phiên

Phiên bản Windows mới an toàn hơn nhưng điều này không thể cắt đứt những cuộc tấn công web.

Windows Vista hứa hẹn bảo mật tốt hơn và Microsoft cũng vừa xây dựng những biện pháp bảo mật "cao tay" hơn nữa vào phiên bản hệ điều hành mới nhất của hãng. Nhưng các làn sóng tội phạm trực tuyến cũng đang có kế hoạch giữ cho các chương trình ác ý của chúng tồn tại và lớn mạnh.

Hiện đã có vài phần mềm ác ý hoạt động được trong Vista, một phần bởi vì Microsoft cố gắng làm cho một số chương trình cũ trên XP chạy được trên Vista. Theo một chuyên gia, trong khoảng vài trăm mẫu phần mềm ác ý mà công ty ông thường xuyên phải xử lý trên XP thì có khoảng 30% trong số này chạy được trên Vista mà không cần chỉnh sửa lại. Số còn lại chỉ cần chỉnh sửa một chút là chạy được. Các cảnh báo giả yêu cầu người dùng khẳng định kích hoạt Windows (xem hình) hay tìm kiếm chi tiết thẻ tín dụng hoặc thẻ ngân hàng và một số mẹo phổ biến khác đánh vào tâm lý người dùng sẽ trở nên tinh vi và lan rộng hơn để vượt qua được bảo mật của Vista. Bạn sẽ còn thấy nhiều mối đe doạ nền web có thể lấy cắp dữ liệu qua bất cứ trình duyệt nào.

Một tấn công gần đây dùng cửa sổ pop-up Windows Activation rất thuyết phục để lừa người dùng cung cấp thông tin nhạy cảm. Xu hướng này được dự báo sẽ xuất hiện nhiều

Vista tạo cho mình vỏ bọc cứng hơn đối với các phần mềm ác ý cài đặt lén lút vào máy tính. Ví dụ, phần mềm ác ý có thể bị chặn ngay ở cửa User Access Control (UAC) của Vista thì bạn có thể dự

đoán rằng cách tấn công dựa trên tâm lý người dùng sẽ trở nên phổ biến hơn. UAC cố chặn đường đi của malware bằng cách từ chối, không cho chúng tự xâm nhập vào các tập tin hệ thống quan trọng. Nếu một người dùng hay một chương trình cố thực hiện thay đổi nào đó trong hệ thống thì cửa sổ pop-up hiện ra yêu cầu người dùng phải "phê chuẩn" hành động này.

Vấn đề là các tác giả malware biết rằng nếu họ có thể làm cho người dùng nhấn được nút OK chỉ một lần thì malware có thể "giải quyết" được UAC. Một chuyên gia ngạc nhiên là ông chưa thấy chương trình tấn công nào ép các nhắc nhở UAC chạy ào ào như tống thư rác trên PC của bạn, có lẽ vì người dùng đã quen "OK" đại cho nhiều dạng pop-up trước đây.

Tệ hơn nữa, UAC chỉ cho 2 tùy chọn cài đặt - chặn hoàn toàn chương trình hoặc cho phép hoàn toàn chương trình - đây là điều mà nhiều chuyên gia bảo mật cho là lỗi thiết kế. Vì vậy nếu tin tặc có thể lừa được người dùng để thực thi cài đặt chẳng hạn bằng một pop-up đầy thuyết phục hoặc bằng cách ẩn nấp trong screensaver hoặc trong các tập tin tải về thông thường thì coi như đã chiếm được hệ thống của bạn. UAC coi như "đứt bóng".

Hiểm họa từ trình duyệt

Các chuyên gia bảo mật cũng cảnh báo rằng bạn sẽ thấy nhiều mối hiểm họa trên nền web hơn nữa dù cho có chế độ Protected Mode trong Internet Explorer 7 của Vista. Protected Mode là một cách tiếp cận thông minh, giới hạn khả năng của IE, hoặc một lỗ rò rỉ nào đó có thể chiếm quyền kiểm soát IE để xâm lấn tiếp các phần còn lại của hệ điều hành, thậm chí vượt ngoài phần kiểm soát của UAC. Nhưng nhiều kiểu tấn công dựa trên web có thể hoạt động thậm chí trong cả Protected Mode, dùng mã JavaScript ác ý để lấy cắp dữ liệu của bạn từ các tài khoản trực tuyến (như một cuộc bán đấu giá giả mạo trên eBay gần đây nhưng đưa người dùng đến trang web lừa đảo). Những tấn công này không cần truy cập tập tin hệ thống mà chúng chỉ cần lấy dữ liệu qua trình duyệt của bạn.

Những kiểu tấn công như vậy vừa có những hạn chế lại vừa mạnh hơn kiểu tấn công dạng cài một tập tin malware lên máy vì "vòi bạch tuộc" của chúng có thể chạm đến nhiều trình duyệt và nhiều hệ điều hành nhưng chấm dứt khi bạn đóng trình duyệt.

BA CÁCH TỰ BẢO VỆ

1. Hãy nhạy bén để đối phó với kiểu lừa đánh vào tâm lý người dùng. Trên hết, bạn đừng tin vào bất kỳ tập tin e-mail đính kèm nào thậm chí ngay cả từ người mà bạn biết. Đường link trong e-mail cũng vậy, bạn nên luôn luôn dùng bookmark hoặc gõ vào địa chỉ URL để truy nhập tài khoản

của mình.

2. Dùng mật mã mạnh, khó đoán cho mỗi trang web quan trọng. Nhiều mật mã sẽ giảm được rủi ro đánh cắp tất cả tài khoản và dịch vụ của bạn. Và những công cụ miễn phí tuyệt vời như Password Hash của Stanford có thể thay cho trí nhớ để quản lý mật mã.

3. Hãy thử trước những chương trình tải về mà bạn không chắc chắn. Tải tập tin mà bạn nghi ngờ (nếu từ 10MB trở xuống) lên Virustotal.com, nó sẽ quét tập tin bằng nhiều engine chống virus để lọc malware mà chương trình chống virus đơn lẻ có thể bỏ sót.