LỖI BẢO MẬT IE LẠI ĐƯỢC DÙNG ĐỂ PHÁT TÁN ADWARE

Hãng bảo mật iDefense cảnh báo đã có khoảng hơn một triệu người dùng MySpace.com cùng như một số trang web khác đã bị nhiễm một phần mềm quảng cáo rất nguy hiểm. Phần mềm quảng cáo nói trên được phát tán chủ yếu thông qua một quảng cáo cho

Hãng bảo mật iDefense cảnh báo đã có khoảng hơn một triệu người dùng MySpace.com cùng như một số trang web khác đã bị nhiễm một phần mềm quảng cáo rất nguy hiểm. Phần mềm quảng cáo nói trên được phát tán chủ yếu thông qua một quảng cáo cho trang web deckoutyourdeck.com xuất hiện trong trang quản lý tài khoản trên trang web MySpace, Ken Dunham - một chuyên gia của iDefense - cảnh báo. Phần mềm quảng cáo nói trên khai thác lỗi bảo mật trong cách trình duyệt Internet Explorer xử lý các tệp tin ảnh Windows Metafile (WMF). Lỗi bảo mật WMF đã được cảnh báo từ tháng 12/2005 sau khi tin tặc phát tán một bức ảnh WMF độc hại thông quan email, tin nhắn tức thời và trang web. Nếu người dùng mở tệp tin WMF đó ra, các đoạn mã độc hại nhúng trong đó có thể cho phép tin tặc đoạt quyền kiểm soát hệ thống của người dùng. Tính đến nay đã có tổng cộng 600 trang web nhắm mục tiêu khai thác lỗi bảo mật WMF, Dunham cho biết. Tháng 1 vừa qua, Microsoft đã phát hành bản vá để khắc phục lỗi bảo mật WMF. Tuy nhiên, đáng tiếc là vẫn còn có nhiều hệ thống máy tính người dùng chưa cài đặt các bản vá khiến cho hệ thống của họ vẫn hoàn toàn mở cửa cho tin tặc. Chính vì thế mà các hệ thống chưa cài đặt bản vá đã trở thành mục tiêu dễ bị tấn công nhất. Chỉ cần truy cập vào một trang web có chứa banner quảng cáo của deckoutyourdeck.com, những hệ thống này sẽ bị nhiễm ngay một con trojan. Còn những hệ thống đã cài đặt bản vá lỗi thì sẽ được hệ thống cảnh báo có tệp tin "exp.wmf" được tải về, Dunham cho biết. Một khi con trojan nói trên được kích hợp, nó sẽ điều hệ thống bị nhiễm kết nối tới một loạt các trang web khác để tải về rất nhiều phần mềm độc hại khác, trong đó có phần mềm quảng cáo của PurityScan. Đây là phần mềm liên tục làm bung ra các cửa sổ quảng cáo trên màn hình đồng thời ghi nhận lại mọi hoạt động trực tuyến của người dùng. Phần mềm quảng cáo PurityScan rất khó bị gỡ bỏ, nó yêu cầu phải có kiến thức về kỹ thuật. iDefense ước tính đến nay đã có khoảng 1,07 triệu máy tính bị nhiễm phần mềm độc hại của nói trên, đồng thời cảnh báo người dùng nên nhanh chóng cài đặt các bản cập nhập bảo mật và nâng cấp cập nhật phần mềm bảo mật. Hoàng Dũng