

YAHOO 360 SẼ ĐƯỢC VÁ LỖ TRONG VÒNG 2 NGÀY TỚI

“Đ

“Đây là một lỗi nghiêm trọng”, đại diện Yahoo khu vực Đông Nam Á Jason Coates thừa nhận với VnExpress. Trong khi đó, lỗ hổng này liên tục bị khai thác và nhiều blogger đã trở thành nạn nhân.

Một blogger có nick pclouds sau khi mắc bẫy tự tay xóa hàng chục comment trên site của chính mình đã "tức khí" tự biến thành kẻ phá hoại người khác. Trên blog của mình pclouds viết: Tiếp tay khoe hàng cực đẹp, cấm trẻ em dưới 18 tuổi cũng như trên 40 tuổi. Đây nè! Không coi uổng cả đời. Coi đi rồi .. hối hận... Nói hết sức nghiêm túc. Coi rồi là hối hận đó.

Thực chất, dấu dưới chữ "Đây nè" là đường dẫn đến một website khác chứa mã độc có thể biến bất cứ ai không đề cao cảnh giác sẽ trở thành người tự tay xóa blog của chính mình.

Blog của pclouds và phần comment phía dưới là nạn nhân của người này. Ảnh chụp màn hình.

Blog của người có nick Camanh có số lượng 519 entry, page view lên tới 150.713, số quick comment là 8530, Friend list gồm 296 người, số tin nhắn Invitation trong hòm thư là 417... Sau khi bị lừa và tự xóa mất 200 entry, Camanh ảm ức giải bày: Bị lừa một cú ảo như vậy mất lòng tin với cái mình từng tiếp xúc, cái ảo. Đối với người khác thì chẳng là gì. Đối với tôi nó là một phần cuộc sống.

Trên blog của mình, nạn nhân Camanh viết: Khóc... như một đứa trẻ bị người khác giật lấy 200 trang nhật ký... xé tan... Ảnh chụp màn hình.

Blogger Robbey® cũng bị mất nhiều nội dung thông tin trong ngôi nhà ảo nhưng có cái nhìn lạc quan hơn: Entries bị mất thì tiếc thật. Nhưng cái gì thuộc về mình vẫn là của mình. Suy nghĩ và tình cảm vẫn thế, nằm tại tâm, những người cần đọc cũng đã đọc hết rồi. Mình sẽ tiếp tục blog và backup, để xem ai dai sức hơn ai.

Trong khi đó, người phát hiện lỗi đầu tiên Nguyễn Ngọc Long nhận định rằng chính việc bố trí cơ sở dữ liệu khá chủ quan của Yahoo 360 là để các entry (những phần do chủ nhân của blog viết ra, cần được bảo vệ ở mức an toàn cao nhất) cùng chỗ với các comment (phần do bạn bè của chủ blog viết lên) đã khiến việc khai thác lỗi CSRF trở nên rất nguy hiểm. Đặc biệt là khi còn một trang quản lý comment nữa của Yahoo 360 cũng có lỗi CSRF, cho phép xóa các comment chỉ cần theo số thứ tự mà không cần kèm theo ID định danh đã được mã hóa của từng site. Lợi dụng điều này, kẻ xấu có thể dùng một đoạn mã hiểm ác để xóa toàn bộ nội dung của bất kỳ blog nào.

Nguyễn Hằng - Thùy Hương