TIN TẶC ĐE DỌA MẠNG XÃ HỘI

Các tr

Các trang web mạng xã hội không chỉ thu hút những người lướt Net bình thường mà còn cả những tên tội phạm công nghệ cao. Các chuyên gia bảo mật dự báo đây sẽ là mục tiêu tấn công của loại tội phạm này trong năm 2008.

Các công ty an ninh mạng khuyến cáo bản chất tưởng chừng như thân thiện của những trang này có thể khiến mọi người dễ dàng chia sẻ thông tin và từ đó biến họ thành đối tượng của các cuộc tấn công. Thông tin chi tiết thu được từ các trang này khiến cho việc gửi spam và lừa đảo trực tuyến trở nên dễ dàng hơn.

Không thể phủ nhận rằng năm 2007 là năm những trang xã hội như MySpace, Facebook, Bebo, Orkut phát triển rực rỡ khi hàng triệu người đăng ký thành viên và post những thông tin cá nhân cũng như thú vui sở thích lên mạng.

Nhưng trong năm 2008 những trang này sẽ trở thành đối tượng tấn công của những nhóm tội phạm công nghệ đứng đằng sau phần lớn những vụ án trực tuyến.

Mary Landesman, Nghiên cứu viên an ninh cấp cao tại ScanSafe, cho rằng mạng xã hội trở nên nguy hiểm do 2 nguyên nhân: những công nghệ được áp dụng vào đó và các ứng dụng bên thứ ba.

Vào cuối năm 2007, cư dân mạng Brazil sử dụng trang Orkut của Google là đối tượng tấn công của một loại sâu cố đánh cắp thông tin về tài khoản ngân hàng. Chương trình này cũng cố gắng tấn công vào những máy tính đã bị thỏa hiệp, lan truyền qua những đường link bẫy đặt trên các trang cá nhân của người sử dụng Orkut.

Tội phạm công nghệ cao đang nhắm đến đối tượng là các mạng xã hội (Nguồn: AP)

Các cuộc tấn công khác lại nhằm vào sự phổ biến của những video clip trên những trang như YouTube cũng bằng cách đặt link bẫy ở những trang chiếu phim ngắn.

Lỗ hổng công nghệ trong hệ thống mạng này đi kèm với những vấn đề về lượng thông tin mà mọi người chia sẻ trên các mạng xã hội.

Dữ liệu này cung cấp cho bọn tội phạm những thông tin về tên của những nhân viên tại một công ty, cấu trúc quản trị và các tiến trình xử lý của nó để tạo độ tin tưởng nhắm vào các cuộc tấn công khác. Những thông tin này có thê rất cụ thể và riêng biệt như tên công ty, những sự kiện và nhân viên.

Landesman cho rằng những thông tin trên có thể giúp tin tặc lừa đảo những nhân viên bằng việc giả dạng thành một đồng nghiệp hoặc đối tác kinh doanh.

David Porter, chịu trách nhiệm về an ninh tại Detica, cho biết sự quen thuộc của các trang mạng xã hội giúp mọi người thiết lập mối quan hệ với những người chia sẻ thông tin sở thích của mình cũng đồng nghĩa với việc mọi người đang bất cẩn với thông tin cá nhân của mình. "Đáng chú ý là mọi người sử dụng mạng xã hội đều đăng những thông tin về cuộc sống, đời sống tình cảm, công việc và thói quen cho toàn thế giới trong khi họ lại ngại chia sẻ loại thông tin này với một người lạ gặp trong quán bar. Những thông tin như thế này là cực kỳ quý giá với bọn lừa đảo mạo danh."

Việc chuyển hướng sang các trang xã hội sẽ là một bước tiến mới so với việc tấn công vào các lỗ hổng trong hệ điều hành Windows để chiếm máy tính và đánh cắp dữ liệu.

Theo Paul King, tư vấn an ninh cấp cao cho Cisco, bọn tội phạm còn tiến bộ hơn ở khả năng sử dụng những email lừa đảo để khai thác người dùng. "Nhiều cuộc tấn công không liên quan gì đến lợi dụng. Họ chỉ cần bạn click vào một đường link và không có nguy cơ nào từ việc đó cả."

Một thử thách lớn trong năm 2008 đối với các cá nhân và công ty là chấp nhận và nhận ra những mối nguy hiểm họ đang gặp phải. Tuy nhiên, người sử dụng không nên quá lo lắng về những vấn đề tiềm tàng này vì sử dụng mạng xã hội vẫn còn rất nhiều lợi ích và mặt trái của nó cũng không làm mọi người quá bận tâm.

Kết luận của Paul King là cố gắng kiểm soát được rủi ro hơn là trốn tránh nó.