TROJAN ẨN MÌNH THEO SPAM KHIÊU DÂM

Bọn tội phạm mạng vừa mới phát động một cuộc tấn công lừa đảo qua email mới giả mạo buộc tội người nhận có liên qua đến một trang web khiêu dâm trẻ em. Các chuyên gia bảo mật khẳng định mục tiêu chính của trong vụ tấn công lần này của bọn tội phạm mạng là lừa những

Bọn tội phạm mạng vừa mới phát động một cuộc tấn công lừa đảo qua email mới giả mạo buộc tội người nhận có liên qua đến một trang web khiêu dâm trẻ em. Các chuyên gia bảo mật khẳng định mục tiêu chính của trong vụ tấn công lần này của bọn tội phạm mạng là lừa những người nhận email tải về các phần mềm độc hại giúp chúng kiểm soát hệ thống hoặc ăn cắp các thông tin cá nhân bí mật của họ. Những bức email nói trên đều có chung một tiêu đề "CP investigation was started" (Cuộc điều tra tệ nạn khiêu dâm trẻ em đã bắt đầu) và có nội dung là địa chỉ email của người nhận đã bị phát hiện tồn tại trong cơ sở dữ liệu của một trang web chuyên về khiêu dâm trẻ em. Trang web này đã bị Hiệp hội những người bảo vệ trẻ em (ASACP) phát hiện được trong một cuộc điều tra. Trích đoạn nội dung email đó như sau:

"I'd like to inform you that investigating activity of the o-ne of child porno sites; we found e-mails data base, in which was your e-mail . In view of this, I have two versions: either you are the client of this shop, or your e-mail appeared there accidentally. I sincerely hope that it was accidental coincidence and believe that you are interested in this version as well. If you show a good will, make modest, voluntary donation o-n our site [URL removed] I will be convinced in your being not implicated in this business." "Tôi muốn thông báo cho bạn biết một thông tin là trong khi tiến hành điều tra các trang web khiêu dâm trẻ em, tôi đã phát hiện ra rất nhiều các địa chỉ email, trong đó có địa chỉ email của bạn … Trong trường hợp này, tôi cho rằng bạn có thể là khách hàng của trang web khiêu dâm nói trên hoặc địa chỉ email của bạn chỉ tình cờ xuất hiện trong cơ sở dữ liệu của trang web đó. Tôi thật sự hi vọng rằng đây chỉ là một trường hợp tình cơ và chắc bạn cũng mong muốn đây chỉ là trường hợp tình cờ. Nếu bạn có thiện chí hãy quyên góp cho trang web của chúng tôi một chút. Đây cũng sẽ là bằng chứng để thuyết tôi là bạn không hề có liên quan đến trang web khiêu dâm đó …"

Trên thực tế đi kèm theo những bức email nói trên là một con trojan có tên là Agent-CPK. Thông tin từ hãng bảo mật Sophos cho biết đây là loại trojan có khả năng thay đổi các thiết lập trình duyệt như bắt cóc trình duyệt, thay đổi trang chủ … Con trojan Agent-CPK thường ẩn mình trong tệp tin có tên "asset576.zip". Giải nén tệp tin này người dùng sẽ nhận được một tệp tin có tên "asset.txt.exe". Nếu nhắp chuột vào tệp tin con trojan sẽ được kích hoạt và lây nhiễm lên hệ thống. "Hiểm hoạ ở đây là người dùng khi nhận được email nói trên thường lo lắng là địa chỉ của họ đã được phát hiện trên một trang web khiêu dâm. Họ sẽ mở email và bị lây nhiễm trojan," Graham Cluley – chuyên gia tư vấn công nghệ cao cấp của Sophos - cảnh báo. ASACP đã đăng thông tin cảnh báo về chiến dịch nói trên lên trang web chính thức của hiệp hội. Hoàng Dũng