

THƯ RÁC HÌNH THƯA VẮNG, THƯ RÁC PDF NỔI LÊN

Sau mộ

Sau một thời gian hoành hành, số lượng thư rác hình đã giảm hẳn trong vài tuần trở lại đây. Nhưng cùng lúc ấy, một loại hình thư rác mới lại nổi lên, với file đính kèm dạng PDF để dụ người dùng mua cổ phiếu của một công ty nào đó.

"Lượng thư rác hình sụt giảm là do các hãng bảo mật đã nhanh chóng điều chỉnh lại sản phẩm của họ. Nếu trước kia, thư rác hình dễ dàng qua mặt bộ lọc thì bây giờ, chúng đã bị chặn lại với tỷ lệ khá cao", ông Paul Henry, Phó chủ tịch công nghệ của Secure Computing cho biết.

Lúc trước, sở dĩ thư rác hình lừa được bộ lọc là vì bên trong nội dung của email đã được nhúng thêm một hình ảnh. Thủ thuật này khiến cho bộ lọc - vốn dựa vào những tổ hợp vô nghĩa hay xuất hiện trong thư rác để xác định đâu là email hợp pháp và đâu là email ngoài ý muốn - không thể giải mã được.

Đầu năm 2007, số lượng thư rác hình chiếm quá nửa tổng số thư rác luân chuyển trên mạng. Nhưng bắt đầu từ tháng 7, chúng chỉ còn chiếm 38% và hiện tại đã giảm xuống còn vèo vèo 19%.

Số liệu từ Symantec cũng cho ra kết luận tương tự. Theo đó, lượng thư rác hình bắt đầu giảm từ tháng 5, liên tục cho đến thời điểm này.

"Các phần mềm chống thư rác, danh sách đen và các bộ lọc đã làm rất tốt công việc của chúng. Giờ là lúc hacker tìm kiếm một hướng đi mới để gây khó dễ cho giới bảo mật", Symantec dự đoán.

Sóng này chưa qua, sóng khác đã tới

Bắt đầu thế chỗ thư rác hình chính là thư rác PDF, dạng thư rác mà spammer sử dụng file đính kèm dạng PDF - định dạng mà hầu hết bộ lọc đều không đọc được. Nội dung của nó là thuyết phục người nhận mua cổ phiếu.

Cho tới nay, các hãng bảo mật mới ghi nhận được 2 loại thư rác PDF: Một loại trông rất chuyên nghiệp, dưới dạng newsletter và đã phát tán tới... 5 tỷ lần chỉ trong vòng vài ngày đầu tiên. Loại thứ hai trông đơn giản hơn, với nội dung ca ngợi một cổ phiếu của Đức.

"Chỉ trong vòng 10 ngày cuối tháng sáu, loại thứ hai đã được gửi tới cho hơn 30 triệu người dùng", Symantec cho biết.

Vì mới xuất hiện, thư rác PDF chưa thể đạt đến số lượng "đỉnh cao" như thư rác hình. Tính đến đầu tháng 7, chúng mới chỉ chiếm khoảng 4% tổng lượng thư rác gửi đi - tuy nhiên, rõ ràng là độ hiểm độc và tinh vi của nó cao hơn nhiều.

"Thư rác PDF cho thấy spammer không ngừng sáng tạo và cải tiến kỹ thuật của chúng. Cuộc chiến giữa spammer với giới bảo mật luôn luôn là mèo vờn chuột. Công cụ chống thông minh một thì spammer tỏ ra sáng tạo 10", bà Sharon Finney, Giám đốc Bảo mật thông tin của Dekalb Medical Center tuyên bố.

Trọng Cẩm