THỦ ĐOẠN PHISHING NGÀY CÀNG XẢO QUYỆT HƠN

Tội phạm phishing (lừa đảo trực tuyến) ngày càng sử dụng các cơ chế "social engineering" (lừa đảo dựa trên phản ứng và thói quen thông thường của người dùng) phức tạp và xảo quyệt hơn nhằm ăn cắp thông tin cá nhân hay tài sản sở hữu trí tuệ của

Tội phạm phishing (lừa đảo trực tuyến) ngày càng sử dụng các cơ chế "social engineering" (lừa đảo dựa trên phản ứng và thói quen thông thường của người dùng) phức tạp và xảo quyệt hơn nhằm ăn cắp thông tin cá nhân hay tài sản sở hữu trí tuệ của doanh nghiệp. Đây là kết luận quan trọng nhất trong Báo cáo về phần mềm độc hại toàn cầu 2006 của hãng bảo mật MessageLabs. Trong lĩnh vực bảo mật máy tính, các "social engineering" là một hành vi thu thập hay ăn cắp thông tin bí mật của người khác bằng cách giả mạo một người dùng hoàn toàn hợp pháp. "Quản lý mối quan hệ nạn nhân?"

Nguồn: microsoft.com

Báo cáo của MessageLabs cảnh báo: Ngày mà người dùng có thể nhận diện được những dạng thức email lừa đảo phishing đang đến gần. Nhưng như thế chưa phải là đã hoàn toàn triệt con đường sống của bọn tội phạm mạng. Giờ đây tội phạm phishing đang phát triển một hướng tiếp cận nạn nhân được cá nhân hoá bằng cách bắt chước kỹ thuật quản lý quan hệ khách hàng hay được ứng dụng trong các doanh nghiệp hợp pháp. Chiến thuật mới của bọn tội phạm mạng được đặt tên là "Kỹ thuật quản lý mối quan hệ nạn nhân" (victim relationship management). "Vụ tấn công phishing mới nhất có sử dụng kỹ thuật social engineering là vụ tấn công vào các trang web mạng xã hội như MySpace nhằm thu thập thông tin cá nhân," Mark Sunner - kỹ sư công nghệ trưởng của MessageLabs – cho biết. "Trong vụ tấn công này, nạn nhân sẽ nhận được một email cá nhân giả mạo từ ngân hàng của họ yêu cầu họ sửa đổi lại thông tin về địa chỉ mã vùng điện thoại". MessageLabs đã ghi nhận được sự gia tăng mạnh mẽ của hình thức tấn công như thế này kể từ tháng 12/2005. Virus cũng vì mục tiêu lừa đảo

Nguồn news.softpedia.com

Báo cáo của MessageLabs cũng cho biết spam và virus cũng có sự gia tăng đáng kể. Đây là một kết quả đã được dự báo trước vì sự bùng nổ của virus đều có liên hệ trực tiếp tới các vụ tấn công spam hay lừa đảo trực tuyến. Bọn tội phạm mạng thường sử dụng trojan để "tuyển mộ" thêm những zombie – các PC bị chiếm quyền điều khiển - nhằm xây dựng hệ thống các botnet phục vụ cho mục đích tấn công spam và lừa đảo trực tuyến. Đỉnh điểm của các hoạt động virus độc hại là vào mùa hè năm 2004. Tại thời điểm này có lúc đã xuất hiện các hệ thống botnet với hơn 100.000 zombie PC. Tuy nhiên, hiện số lượng các zombie PC của các mạng botnet đã giảm xuống con số 20.000 nhằm tránh bị phát hiện. Nhưng ngược lại ngày càng có nhiều người trở thành nạn nhân của những vụ tấn công nhỏ lẻ có mục tiêu cụ thể hơn. Lấy ví dụ, trong số 321 e-mail được MessageLabs theo dõi thì chỉ có 1 e-mail là spam. Còn các doanh nghiệp lại trở thành nạn nhân của những con trojan rất xảo quyệt ẩn mình trong các tệp tin Microsoft Office giả mạo được gửi đi từ một nguồn rất đáng tin cậy. Hầu hết những vụ tấn công vào doanh nghiệp đều có mục tiêu rất cụ thể nhằm đánh cắp quyền sở hữu trí tuệ tài sản hoặc nhằm mục tiêu gián điệp kinh doanh. Đâu là giải pháp Vậy chúng ta phải làm thế nào để chống lại các hiểm hoạ lừa đảo phishing đang ngày càng gia tăng mạnh mẽ? Ông Mark Sunner khẳng định: Vấn đề ở đây là trong khi bọn tội phạm mạng đang ngày càng ứng dụng các kỹ thuật tấn công phức tạp thì các hãng bảo mật vẫn còn dựa trên mô hình kinh doanh đã có 20 năm tuổi để bảo vệ người dùng. Nói cách khác: Các hãng bảo mật đã chậm chân hơn bọn tội phạm mạng. Các giải pháp lọc chặn cần phải được thực hiện ở cấp độ mạng Internet để ngăn chặn các e-mail phishing không thể được gửi đến hòm thư của người dùng. "Yếu tố con người là yếu tố yếu nhất trong chuỗi mắt xích bảo mật. Nhưng thẳng thắn mà nói, chúng ta đã hoàn toàn không công bằng khi đặt một gánh nặng trách nhiệm như vậy cho người dùng," Sunner nói. "Chúng ta cần áp dụng nhiều giải pháp chặn lọc ở cấp độ cao hơn nữa để ngăn chặn e-mail phishing vươn vòi bạch tuộc đến người dùng". Trang Dung