

Cảnh báo lừa đảo qua mã QR

11:19 29/10/2024

Các ngân hàng và cơ quan quản lý đang cảnh báo về dạng lừa đảo qua mã QR - còn được gọi là “quishing”. Đáng chú ý, quishing đang vượt qua các biện pháp phòng thủ mạng của doanh nghiệp và ngày càng lừa được khách hàng cung cấp thông tin tài chính của họ.

Theo Financial Times, các tổ chức cho vay như Santander, HSBC và TSB đã cùng với Trung tâm An ninh mạng Quốc gia Vương quốc Anh và Ủy ban Thương mại Liên bang Hoa Kỳ (FTC) đang bày tỏ lo ngại về sự gia tăng của các mã QR giả mạo được triển khai cho các chiến dịch gian lận tinh vi.

Lừa đảo qua mã QR ngày càng gây tổn kém cho các công ty

Loại hình lừa đảo qua email mới này thường liên quan đến việc tội phạm gửi các mã QR trong các tệp PDF đính kèm. Các chuyên gia cho biết chiến lược này hiệu quả vì những tin nhắn này thường vượt qua các bộ lọc an ninh mạng của doanh nghiệp — phần mềm thường đánh dấu các liên kết trang web độc hại, nhưng thường không quét các hình ảnh trong tệp đính kèm.

“Điều hấp dẫn đối với tội phạm là nó vượt qua mọi rào cản về an ninh mạng và cũng bỏ qua các sản phẩm của chúng tôi,” ông Chester Wisniewski, cố vấn cao cấp tại công ty phần mềm bảo mật Sophos, cho biết.

Nghiên cứu của IBM cho thấy các cuộc tấn công “lừa đảo” — trong đó kẻ lừa đảo gửi email nhắm mục tiêu với các liên kết độc hại — đang ngày càng tổn kém cho các công ty, với chi phí trung bình toàn cầu cho một vụ vi phạm dữ liệu tăng gần 10% lên 4,9 triệu USD vào năm 2024.



Mã QR chứa dữ liệu, chẳng hạn như URL hoặc thông tin thanh toán, dưới dạng mã nhị phân. Được phát minh bởi công ty Denso Wave của Nhật Bản vào năm 1994 như một công cụ theo dõi các bộ phận ô tô, các mã này được thiết kế để các loại máy móc có thể đọc nhanh, đặc biệt là điện thoại thông minh, nhưng thường thì con người không thể đọc được các mã này.

Mặc dù hầu hết các điện thoại thông minh hiển thị một bản xem trước ngắn về URL chứa trong mã QR được quét, các nhà nghiên cứu cho biết rằng thông báo pop-up này thường không đủ để người dùng có thể phát hiện ra rằng một liên kết có thể là giả mạo.

“Những cuộc tấn công này tận dụng thực tế rằng các mã QR, theo bản chất, rất khó để diễn giải một cách trực quan, vì vậy nạn nhân thường không biết họ đang được chuyển đến đâu cho đến khi quá muộn,” ông Amir Sadon, giám đốc nghiên cứu tại công ty tư vấn an ninh mạng Sygnia, cho biết.

Các nhà chức năng cảnh báo lừa đảo QR CODE

Các ngân hàng cho biết rằng sự phổ biến của loại hình lừa đảo này đã gia tăng kể từ khi mã QR trở nên phổ biến trong đại dịch Covid-19, khi chúng được sử dụng để hiển thị mọi thứ từ hộ chiếu vaccine đến thực đơn nhà hàng. “Chắc chắn đây là một xu hướng đang gia tăng”, bà Steph Harrison, quản lý hoạt động gian lận cao cấp tại TSB, cho biết.

Một cuộc khảo sát của công ty phần mềm bảo mật McAfee vào tháng 5 cho thấy hơn một phần năm tất cả các cuộc lừa đảo trực tuyến ở Vương quốc Anh có thể xuất phát từ mã QR. Số lượng báo cáo về các vụ lừa đảo mã QR ở Vương quốc Anh đã tăng gấp đôi trong năm đến tháng 8 năm 2024, theo Action Fraud.

Ủy ban Thương mại Liên bang Hoa Kỳ, cùng với nhiều cơ quan địa phương trên khắp Vương quốc Anh, cũng đã cảnh báo trong năm nay về một loại lừa đảo “quishing” cụ thể nhắm vào tài xế, bao gồm các trường hợp mà các nhãn dán dẫn đến các trang web giả mạo đã được dán lên trên các mã QR hợp pháp được sử dụng để thanh toán đỗ xe.

Các liên kết này có thể dẫn người dùng đến một trang web sai và yêu cầu họ nhập thông tin cá nhân, hoặc dẫn họ đến việc tải xuống phần mềm độc hại. Thậm chí tồi tệ hơn, bà Harrison cho biết, “bạn cũng có thể bị phạt vì thực sự không có vé đỗ xe.”

Nạn nhân cũng đã báo cáo về các mã QR giả mạo được đặt lên trên các mã hợp pháp tại các điểm sạc xe điện, nhà ga xe lửa và bàn nhà hàng.

Tuy nhiên, các nhà nghiên cứu cho biết rằng các cuộc lừa đảo “quishing” thường được triển khai qua email — một mối đe dọa đã đặt áp lực lên các nhà cung cấp an ninh mạng để điều chỉnh các biện pháp phòng ngừa trực tuyến của họ.

“Ngày nay, gần như không có sản phẩm an ninh mạng nào kiểm tra các tệp đính kèm,” ông Wisniewski nói. “Nếu điều này tiếp tục là một vấn đề, tôi đoán rằng ngành công nghiệp sẽ phải nghiên cứu bổ sung thêm việc quét các tệp đính kèm, nhưng điều này sẽ làm chậm quá trình gửi email và cũng sẽ làm cho mọi thứ trở nên đắt đỏ hơn”.

PV