TẠP CHÍ ĐIỆN TỬ
THƯƠNG HIỆU & CÔNG LUẬN

Hacker đẩy mạnh tấn công vào các hệ thống ngân hàng, máy ATM, dịch vụ thanh toán…

09:39 21/08/2018

Ngày 17/8, hãng bảo mật Kaspersky Việt Nam cho hay trong quý II năm 2018 vừa qua, hacker đã gây hoang mang cho nhiều người sử dụng dịch vụ tài chính, với 21,1% các cuộc tấn công nhắm vào các ngân hàng, 8,17% vào các cửa hàng trực tuyến và 6,43% vào hệ thống thanh toán. Các kết quả trên cho thấy người dùng cần đặc biệt quan tâm đến bảo mật khi lướt internet để bảo vệ tài sản.

Các chuyên gia bảo mật cho hay những cuộc tấn công nhắm vào khách hàng của các tổ chức tài chính như ngân hàng, hệ thống thanh toán và các giao dịch mua bán trực tuyến sẽ là một xu hướng lâu dài đối với tội phạm mạng trong đó các hành vi trộm cắp tiền bạc và cả dữ liệu cá nhân sẽ ngày càng thường xuyên hơn. Bằng cách tạo ra các trang giả mạo ngân hàng, thanh toán hoặc các trang mạng mua sắm, kẻ xâm nhập có thể cướp thông tin nhạy cảm từ các nạn nhân như tên, mật khẩu, địa chỉ email, số điện thoại, số thẻ tín dụng và mã PIN mà họ không hề hay biết.



(Ảnh minh họa)

Bên cạnh đó vào ngày 15/8 vừa qua, các phương tiện truyền thông quốc tế cũng cho hay Cục Điều tra Liên bang Mỹ (FBI) vừa cảnh báo các ngân hàng về nguy cơ bọn tội phạm mạng phối hợp thực hiện một cuộc tấn công nhắm vào các máy rút tiền tự động (ATM) khắp thế giới. Một khi vụ tấn công xảy ra, hàng triệu USD có thể bị đánh cắp trong vòng vài giờ. Theo FBI, tội phạm có thể tấn công trong vài ngày tới đây và thường thì những vụ tấn công loại này xảy ra vào cuối tuần, thời điểm các ngân hàng đóng cửa. Theo các chuyên gia an ninh mạng, bọn tội phạm có thể sử dụng mã độc để truy xuất thông tin thẻ ngân hàng của khách hàng. Sau đó hacker sẽ xóa bỏ các biện pháp chống gian lận như hạn chế số lượng tiền rút ra từ ATM để có thể ra tay đánh cắp toàn bộ số tiền có trong đó.

Còn Trung tâm Ứng cứu khẩn cấp máy tính quốc gia (VNCERT) đầu tháng 8 vừa qua cũng cho biết thời gian gần đây, trung tâm đã ghi nhận các hình thức tấn công có chủ đích của tin tặc nhắm vào hệ thống thông tin của một số ngân hàng và hạ tầng quan trọng quốc gia tại Việt Nam. Với hình thức tấn công có chủ đích này, tin tặc đã tìm hiểu kỹ về đối tượng và thực hiện các thủ thuật lừa đảo, kết hợp với các biện pháp kỹ thuật cao để qua mặt các hệ thống bảo vệ an toàn thông tin (ATTT) của các ngân hàng và các tổ chức hạ tầng quan trọng nhằm chiếm quyền điều khiển máy tính của người dùng, qua đó tấn công các hệ thống máy tính nội bộ chứa thông tin quan trọng khác. Mục đích chính của tin tặc là đánh cắp các thông tin quan trọng của ngân hàng và các tổ chức hạ

tầng quan trọng. Với việc sử dụng các kỹ thuật cao để tấn công, các hệ thống bảo vệ ATTT của ngân hàng hoặc các tổ chức hạ tầng quan trọng sẽ khó phát hiện kịp thời, giúp tin tặc duy trì quyền kiểm soát hệ thống thông tin. Để ngăn chặn các cuộc tấn công này, VNCERT đề nghị các ngân hàng và tổ chức hạ tầng quan trọng quốc gia tại Việt Nam thực hiện gấp các biện pháp phòng chống để kịp thời phát hiện và ngăn chặn cuộc tấn công có chủ đích.

Trước tình hình này, các chuyên gia khuyên người dùng Việt Nam nên thực hiện các biện pháp sau đây để bảo vệ bản thân và tránh khỏi lừa đảo:

●Luôn kiểm tra địa chỉ liên kết và email của người gửi trước khi nhấp vào.

●Trước khi nhấp vào bất kỳ liên kết nào, hãy kiểm tra xem địa chỉ liên kết được hiển thị và liên kết thực tế (địa chỉ thực mà liên kết sẽ đưa bạn đến) có giống nhau hay không.

● Chỉ sử dụng kết nối an toàn, đặc biệt là khi bạn truy cập các trang web nhạy cảm. Để phòng ngừa tối thiểu, không sử dụng Wi-Fi không xác định hoặc công cộng mà không có mật khẩu bảo vệ. Để bảo vệ tối đa, hãy sử dụng các giải pháp VPN để mã hóa các truy cập của bạn. Và hãy nhớ nếu bạn đang sử dụng kết nối không an toàn, tội phạm mạng có thể chuyển hướng bạn một cách vô hình đến các trang lừa đảo.

● Kiểm tra kết nối HTTPS và tên miền khi bạn mở một trang web. Điều này đặc biệt quan trọng khi bạn đang sử dụng các trang web chứa dữ liệu nhạy cảm - chẳng hạn như trang web cho ngân hàng trực tuyến, cửa hàng trực tuyến, email, trang web truyền thông xã hội,...

● Không bao giờ chia sẻ dữ liệu nhạy cảm của bạn, chẳng hạn như thông tin đăng nhập và mật khẩu, dữ liệu thẻ ngân hàng,... với bên thứ ba. Các công ty chính thức sẽ không bao giờ yêu cầu dữ liệu như thế này qua email.

● Sử dụng giải pháp bảo mật đáng tin cậy với các công nghệ chống lừa đảo dựa trên hành vi để phát hiện và chặn các cuộc tấn công spam và lừa đảo.

Bảo Ngọc