TROJAN ĂN CẮP TÀI KHOẢN YM ĐỂ LỪA ĐẢO TẠI VIỆT NAM

Bằng n

Bằng những tài khoản Yahoo Messenger đánh cắp được, kẻ lừa đảo trò chuyện với bạn bè nạn nhân, khai thác thông tin và nhờ mua hộ thẻ nạp tiền điện thoại. Đồng thời, chúng phát tán link website có chứa mã độc để tiếp tục phạm tội.

Anh Vũ Trung Nghĩa, một nạn nhân của trò lừa đảo trực tuyến mới này, đã gửi e-mail chia sẻ với VnExpress về việc anh nhận được đường link download file http://files.myopera.com/em .../tracnghiem.exe từ người bạn. Một thời gian sau khi chạy file này, anh bất ngờ nhận được lời nhắn về việc thanh toán những thẻ cào điện thoại nhờ mua trước đó mà anh không hề biết. Vài người khác than phiền bị mất mật khẩu e-mail sau khi anh "dùng nhờ vì hộp thư tớ đầy quá" dù anh chẳng mượn của ai. Hỏi lại Nghĩa mới biết những "yêu cầu giúp đỡ" trên đều xuất phát từ tin nhắn từ nickname YM của mình mà anh không biết.

Theo mô tả của Nghĩa, người bạn của anh có kể lại rằng hacker cũng có "khúc dạo đầu" thăm hỏi, lân la dò chuyện rồi mới đề nghị mua giúp thẻ cào hoặc sim điện thoại có mệnh giá từ 300 - 500 nghìn đồng rồi gửi dãy số bí mật cho hắn. Một vài người đã trở thành nạn nhân vì tưởng bạn mình đang gặp khó khăn thật.

Phân tích của Trung tâm an ninh mạng Bách Khoa (BKIS) cho thấy công cụ phạm tội là các phần mềm Trojan dạng keylogger (ghi mã bàn phím và chuột) có kích thước siêu nhỏ, chỉ khoảng 40 KB, được cài sẵn trên website của hacker và ngụy trang dưới dạng 1 file ca nhạc hoặc trắc nghiệm giải trí. Khi nạn nhân chạy chương trình, Trojan sẽ xâm nhập vào máy tính dưới cái tên explore.exe trong thư mục hệ thống, đồng thời tạo thêm file explorer.dll để ghi lại toàn bộ các thao tác bàn phím và chuột của người sử dụng, thay đổi thông số trong hệ thống Registry của Windows để tự động chạy mỗi lần khởi động. Sau khi kiểm soát được hệ thống, Trojan tự động gửi toàn bộ thao tác của người dùng vào e-mail của hacker.

"Như vậy, hacker có toàn bộ tài khoản và mật khẩu mà nạn nhân đang dùng trên máy tính của mình chứ không chỉ Yahoo Messenger", ông Vũ Ngọc Sơn, Trưởng phòng virus BKIS, phân tích. "Có được cả kho mật khẩu, tin tặc dò tìm trên máy tính của chúng và tiến hành các thủ đoạn lừa đảo".

Ông Sơn cho biết Trojan này không phức tạp về kỹ thuật, nhưng "mánh lừa" của những kẻ sử dụng chúng thì đáng kể bởi dễ dàng nói chuyện mà không gây nghi ngờ cho nạn nhân. Trò lừa

đảo này mới xuất hiện và chưa có thống kê chính thức. Tuy nhiên, các chuyên gia an ninh mạng cũng đề xuất người dùng nên cảnh giác hơn trong thời gian sắp tới vì các biến thể của chúng.

Hưng Hải