

Công an TP. Hồ Chí Minh cảnh báo nguy cơ mã độc đánh cắp thông tin ngân hàng

12:03 11/12/2023

Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao - Công an TP. Hồ Chí Minh (PA05) vừa phát hiện tình trạng các loại mã độc đánh cắp thông tin, mã hóa dữ liệu người dùng - thông qua các ứng dụng giả mạo. Tình trạng này đang có dấu hiệu tăng cao vào dịp cuối năm 2023.

Thủ đoạn lừa đảo là sử dụng câu chuyện nguy trang hợp lý để dẫn dụ nạn nhân cài đặt ứng dụng mã độc, như: Giả danh Công an khu vực yêu cầu đăng ký định danh mức 2 VNeID, hay cập nhật thông tin bảo hiểm xã hội (BHXH) trên ứng dụng VSSID để được hưởng quyền lợi bảo hiểm lao động ở mức cao. hay giả mạo nhân viên ngân hàng đề nghị tạo tài khoản ngân hàng mới, mở thẻ tín dụng để được hưởng hạn mức ưu đãi.

Đặc biệt, các đối tượng đã lợi dụng lỗ hổng trên một số trang mạng điện tử có đuôi .gov.vn hay .com.vn để cài backlink download ứng dụng (app) làm nạn nhân tưởng nhầm đây là ứng dụng của các trang mạng chính thống của cơ quan Nhà nước nên yên tâm, chủ quan tải và cài đặt trên điện thoại (smart phone) hoặc máy tính (pc) của cá nhân, công ty mình.



Công an TP. Hồ Chí Minh cảnh báo nguy cơ mã độc đánh cắp thông tin ngân hàng

Khi đó, mã độc lây nhiễm trên thiết bị, nó sẽ giám sát hoạt động của thiết bị. Khi nạn nhân mở ứng dụng trong danh sách mục tiêu, nó sẽ hiển thị giao diện đăng nhập giả mạo chèn lên giao diện thật để đánh lừa người dùng tương tác đăng nhập.

Sau đó, thông tin đăng nhập của người dùng vào ứng dụng Internet Banking sẽ được mã độc gửi về cho đối tượng. Đối với các dòng smartphone chạy hệ điều hành Android, mã độc có thể không cần người dùng cấp quyền truy cập danh bạ, camera, micro,... điện thoại mà vẫn có thể can thiệp vào hệ thống điện thoại.

Thời gian qua, đã có nhiều nạn nhân ở TP. Hồ Chí Minh bị dẫn dụ cài đặt ứng dụng chứa mã độc và bị âm thầm chiếm đoạt rất nhiều tiền trong tài khoản. Sau khi khống chế điện thoại nạn nhân, các đối tượng còn tìm cách khai thác các thông tin trong danh bạ, thư viện ảnh, video clip riêng tư,... để tìm cách khống chế, đe dọa hoặc tiếp tục dẫn dụ các nạn nhân khác là người quen trong danh bạ.

Phòng PA05 cho biết, không chỉ thu thập dữ liệu để đánh cắp tiền, mã độc này còn chặn các tin nhắn và cho phép tin tặc kiểm soát các tài khoản của nạn nhân (Facebook, Email, Zalo...). Mã độc này có thể chứa các tính năng không cho

phép người dùng gỡ cài đặt nó. Vì vậy, để có thể loại bỏ mã độc này, nạn nhân sẽ phải khôi phục cài đặt gốc cho điện thoại của mình.

Công an khuyến cáo người dân tuyệt đối không cài các ứng dụng từ trang web, cổng thông tin bên ngoài mà chỉ nên cài trên kho ứng dụng cửa hàng Play, Apple Store; bật chức năng Google Play Protect, điều này sẽ giúp quét và phát hiện các ứng dụng độc hại hiện có hoặc các ứng dụng mới đang có ý định cài đặt.

Người dân cần thường xuyên nâng cấp hệ điều hành điện thoại và sử dụng phần mềm diệt virus có bản quyền; nên đặt hạn mức số tiền chuyển khoản trực tuyến để kịp thời hạn chế thiệt hại khi bị cài mã độc; nhanh chóng phong tỏa tài khoản cá nhân, công ty nếu nghi vấn và báo cho công an...

Phong Vân