


🕒 12th August 2021

 android mã độc

Phần mềm độc hại này chiếm đoạt các tài khoản mạng xã hội bằng cách lây nhiễm vào các thiết bị Android, cho phép những kẻ tấn công thu thập thông tin từ nạn nhân như ID Facebook, vị trí, địa chỉ email và địa chỉ IP, cũng như cookie và mã thông báo liên kết với tài khoản Facebook.



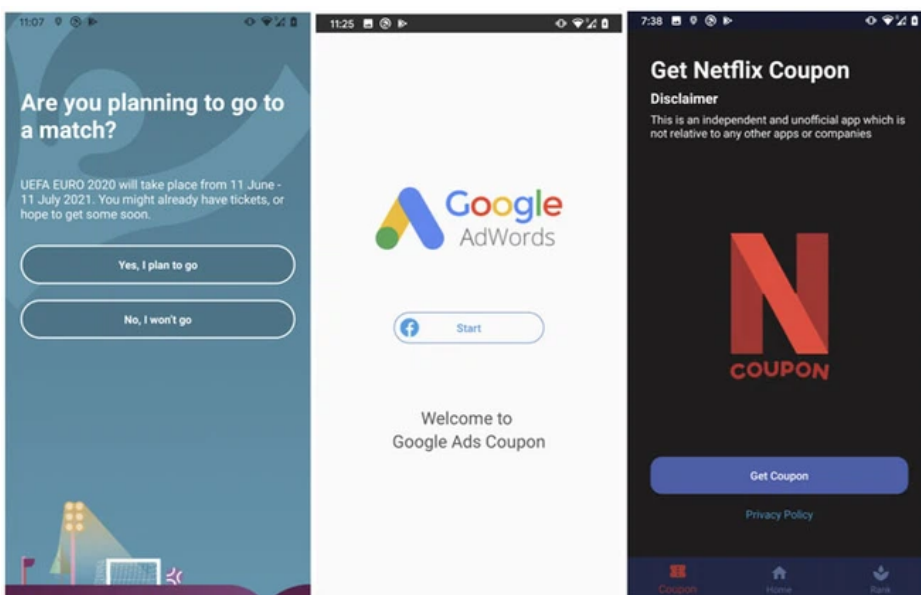
Bản đồ phân phối trojan FlyTrap

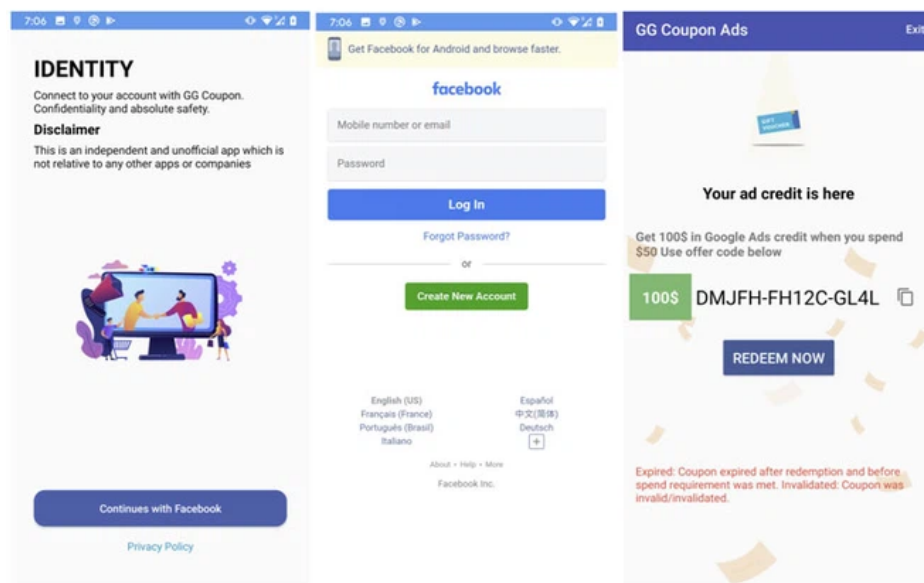
Hoạt động của FlyTrap, đúng như cái tên "Hoa bẫy ruồi", là dựa trên sự tò mò và thích "miễn phí" của người dùng rồi dụ dỗ họ.

Các nhà nghiên cứu Zimperium viết: "Các Facebook bị tấn công này có thể được sử dụng để phát tán phần mềm độc hại bằng cách lạm dụng uy tín xã hội của nạn nhân thông qua tin nhắn cá nhân có liên kết đến Trojan, cũng như tuyên truyền các chiến dịch hoặc thông tin sai lệch bằng cách sử dụng chi tiết vị trí địa lý của nạn nhân".

"Các kỹ thuật xã hội này có hiệu quả cao trong thế giới được kết nối kỹ thuật số và thường được tội phạm mạng sử dụng để phát tán phần mềm độc hại từ nạn nhân này sang nạn nhân khác. Những kẻ xấu đã sử dụng một số chủ đề mà người dùng thấy hấp dẫn như mã voucher dùng Netflix miễn phí, mã phiếu giảm giá Google AdWord và những trò chơi bình chọn cho đội bóng hoặc cầu thủ xuất sắc nhất".

Tất nhiên, không có mã hoặc voucher Netflix hay AdWords miễn phí nào và không có cuộc bỏ phiếu ủng hộ bóng đá nào được thực hiện. Thay vào đó, các ứng dụng độc hại chỉ chờ để lấy thông tin đăng nhập của Facebook khi họ muốn đăng nhập để lấy khuyến mãi. Chúng sẽ thực hiện một nỗ lực cuối cùng để trông có vẻ hợp pháp bằng cách tung ra một thông báo nói rằng phiếu giảm giá hoặc mã đã hết hạn, như trong ảnh chụp màn hình bên dưới.





Các nhà nghiên cứu đã cho rằng phần mềm độc hại này đến từ các nhóm hacker đang hoạt động tại Việt Nam và cho biết những người này có thể phân phối trojan bằng Google Play và các cửa hàng ứng dụng khác.

Đây là các ứng dụng chứa trojan:

*GG Voucher (com.luxcarad.cardid)*

*Vote European Football (com.gardenguides.plantingfree)*

*GG Coupon Ads (com.free\_coupon.gg\_free\_coupon)*

*GG Voucher Ads (com.m\_application.app\_moi\_6)*

*GG Voucher (com.free.voucher)*

*Chatfuel (com.ynsuper.chatfuel)*

*Net Coupon (com.free\_coupon.net\_coupon)*

*Net Coupon (com.movie.net\_coupon)*

*EURO 2021 Official (com.euro2021)*

Google đã được gửi một báo cáo về phần mềm độc hại, đã xác minh nó và xóa tất cả các ứng dụng có liên quan trong cửa hàng, nhưng báo cáo lưu ý rằng ba trong số các ứng dụng vẫn có sẵn trên "kho ứng dụng của bên thứ ba, không an toàn."