

Mã độc đánh cắp tài khoản có thể ‘xuyên thủng’ cơ chế bảo mật 02 lớp

22:55 18/12/2022

Nếu cho rằng các tài khoản được xác thực 02 bước là an toàn tuyệt đối, điều này không đúng với PasswordStealer. Dòng mã độc này lây nhiễm hơn 525.000 máy tính tại Việt Nam trong năm qua, với hơn 15.000 biến thể, đánh cắp và chiếm đoạt tài khoản Facebook, Gmail, tài khoản ngân hàng, ví điện tử... của nạn nhân.



Ảnh minh họa. (Ảnh: internet)

Nhằm vượt qua cơ chế xác thực 02 bước, đầu tiên hacker dùng cookies đánh cắp được để đăng nhập tài khoản. Tiếp đến, chúng sử dụng mật khẩu để xác thực và thực hiện hàng loạt các thao tác như đổi số điện thoại, email khôi phục, đặt mật khẩu mới, đăng xuất hết các thiết bị khác nhằm chiếm đoạt tài khoản.

PasswordStealer chủ yếu phát tán qua các phần mềm crack, phần mềm giả mạo. Tuy nhiên, khảo sát của BKAV cho thấy, 14% người dùng được hỏi vẫn

chọn cài đặt phần mềm từ nguồn bất kỳ tìm được qua Google, thay vì tìm đến nguồn chính thống như website của nhà sản xuất, kho phần mềm đáng tin cậy. 21% người dùng chưa có thói quen kiểm tra virus trước khi mở các file từ internet. Đây là những con số đáng báo động, dẫn đến nguy cơ cao bị nhiễm dòng mã độc này.

PV (t/h)