50 NGÂN HÀNG BỊ LỪA ĐẢO TRỰC TUYẾN KIỂU PHARMING

Trong

Trong khoảng 4 ngày qua, khách hàng của ít nhất 50 tổ chức tài chính tại Mỹ, châu Âu và châu Á - Thái Bình Dương đã bị hacker khai thác thông tin cá nhân bằng một thủ thuật phishing đặc biệt.

Hacker xây dựng trang web riêng giống hệt website của ngân hàng chúng định tấn công. Sau khi người sử dụng bị lừa truy cập vào trang đó, mã độc sẽ khai thác một lỗi nghiêm trọng của Windows (đã được Microsoft phát hành bản sửa chữa năm ngoái).

Hệ thống máy tính chưa được vá sẽ tự động tải một Trojan có tên iexplorer.exe và 5 file khác từ một máy chủ đặt tại Nga. Những trang web này cũng hiển thị một thông báo lỗi và yêu cầu người sử dụng tắt firewall và phần mềm diệt virus.

Thủ thuật trên được gọi là tấn công pharming. Cũng như lừa đảo trực tuyến phishing, hacker trước tiên tạo website giả mạo nhằm dụ người sử dụng tiết lộ thông tin cá nhân. Nhưng với phishing, nạn nhân cần bấm vào đường link trong e-mail để truy cập vào trang web giả, còn kiểu pharming hướng họ tới website chứa mã độc ngay cả khi họ gõ đúng địa chỉ ngân hàng trên trình duyệt. Điều này là do hacker đã thay đổi thông tin địa chỉ của nhà cung cấp dịch vụ Internet thông qua các lỗi phần mềm trên máy chủ của ISP.

Henry Gonzalez, chuyên gia phân tích của hãng bảo mật Websense (Mỹ), khẳng định các website giả, có nguồn gốc từ Đức, Estonia và Anh, đã bị các ISP vô hiệu hóa hôm qua. Tuy nhiên, họ chưa thể xác định có bao nhiêu người đã trở thành nạn nhân trong vụ tấn công này.