WEBSITE .VN BỊ LỢI DỤNG ĐỂ PHISHING NGÂN HÀNG NHẬT

Sau kh

Sau khi tấn công vào máy chủ của hệ thống website Đại Học Duy Tân (Đà Nẵng), hacker đã đưa lên đây một trang lừa đảo mã tài khoản tín dụng (phising) các khách hàng một nhà băng của Nhật.

Ngân hàng Nhật bị website .vn phising?

Khoảng hai ngày nay, CHA...com - một ngân hàng lớn của Nhật phát hiện các khách hàng của mình bị lừa đảo mã số thẻ tín dụng (phising) bởi một trang web đặt tại Việt Nam (tên miền có đuôi .vn).

Sau khi phát hiện sự việc, chiều 6/4/2007 - Ngân hàng CHA...com ngay lập tức liên hệ với VNCERT (Trung tâm Ứng cứu sự cố khẩn cấp máy tính quốc gia - Bộ BCVT Việt Nam) thông qua công ty RSA Cyota (Công ty an ninh mạng mà ngân hàng này thuê dịch vụ) và JPCERT để nhờ giúp đỡ.

Trước sự có mặt của PV VietNamNet, các cán bộ trung tâm VNCERT đã phân tích và khẳng định: Trang web phising bằng cách đưa lên một đường dẫn xuất phát từ website www.dtu.edu.vn/cha...online, với nội dung mời chào khách hàng CHA...com tham gia một chương trình thăm dò khách hàng để nhận thưởng 20 USD.

Và tất nhiên, phía dưới, trang web yêu cầu khách hàng xác nhận lại các thông tin mã số thẻ tín dụng, mật khẩu... của tài khoản mà họ sở hữu tại ngân hàng CHA...com để nhận 20 USD thưởng.

Theo một chuyên viên phòng nghiệp vụ của VNCERT cho biết: "Hệ thống tên miền trong đường link chứa trang phishing mà JPCERT cung cấp đúng là một trang web đang host tại Việt Nam - thuộc hệ thống máy chủ của Đại Học Duy Tân (Đà Nẵng)".

Phản ứng nhanh

Hình ảnh trang web phishing đặt tại dtu.edu.vn dụ người dùng tham gia một chương trình thăm dò khách hàng nhận thưởng 20 USD nhưng phải khai báo các thông tin bí mật về tài khoản tín dụng tại ngân hàng CHA...com (Nhật)

Theo nhận định ban đầu của các chuyên viên VNCERT, máy chủ của Đại Học Duy Tân đã bị hacker tấn công và đưa trang lừa đảo trực tuyến mà bộ phận quản trị chưa hay biết. Bằng biện pháp nghiệp vụ, VNCERT yêu cầu quản trị viên của website ĐH Duy Tân ngay lập tức gỡ trang phising xuống để tránh thiệt hại cho các khách hàng của Ngân hàng CHA...com.

"Chúng tôi cũng đồng thời đưa ra hai yêu cầu khác: Thứ nhất là yêu cầu ban quản trị site này cung cấp toàn bộ source code của trang lừa đảo, nhằm phân tích ngược để biết đó có phải là do các hacker Việt Nam tiến hành hay không. Nếu đúng chúng tôi sẽ giao lại các thông tin này cho bên cơ quan điều tra (C15) để tìm ra thủ phạm. Nếu là hacker nước ngoài, chúng tôi sẽ giao lại cho JPCERT xử lý tiếp phần còn lại."

Đại diện VNCERT nói tiếp: "Yêu cầu thứ ba là chúng tôi đề nghị Ban quản trị website Duy Tân cung cấp các thông tin về thẻ tín dụng mà trang phishing đã lừa đảo được trong những ngày qua. Điều này cũng là đề nghị giúp đỡ từ phía ngân hàng CHA...com và JPCERT, họ muốn biết có những tài khoản nào đã bị lừa đảo để tránh thiệt hại đến mức thấp nhất!".

Theo ghi nhận của PV VietNamNet, việc hạ trang web phising đã được phía ĐH Duy Tân tiến hành ngay lập tức vào khoảng 16h15 chiều 6/7/2007. (tức là chỉ sau khoảng 5 phút có thông báo từ VNCERT).

Ông Đỗ Ngọc Duy Trác, Trưởng phòng nghiệp vụ của VNCERT trong quá trình trao đổi với PV VietNamNet nói: "Theo tôi biết, vấn đề bảo mật tại các website trường ĐH vốn kém hơn nhiều so với khối doanh nghiệp và nhà nước. Đây là thực tế không chỉ ở Việt Nam, nguyên nhân chính do họ không thể đầu tư nhiều chi phí cho hoạt động bảo mật."

"Nếu có thể các trường ĐH nên cố gắng đặt website tại một số nhà cung cấp dịch vụ hosting uy tín, điều này sẽ hạn chế các nguy cơ bảo mật, đồng thời có thể xử lý nhanh và triệt để khi xảy ra sự cố. Bộ phận kỹ thuật cũng nên kiểm tra và backup hệ thống thường xuyên để kiểm soát tình hình tốt nhất." - Ông Trác khuyến cáo.

Thực ra, lần hợp tác này giữa VNCERT và JPCERT không phải là lần đầu tiên, vào tháng 2/2007, ngay sau tết Nguyên Đán, hai đơn vị CERT đã từng phối hợp gỡ bỏ hai trang web khác của Việt Nam hosting tại VNGT và VDC được khẳng định là tiến hành thủ đoạn phising các ngân hàng

Nhật Bản và Canada.

Được biết cũng trong chiều 6/4, VNCERT cũng đã phát công văn điều phối các ISP lớn của Việt Nam ngăn chặn phát tán mã độc thông qua website nhatquang*.t35.com đang có chiều hướng lây lan mạnh thông qua mạng Yahoo Messenger tại Việt Nam.

Thế Phong