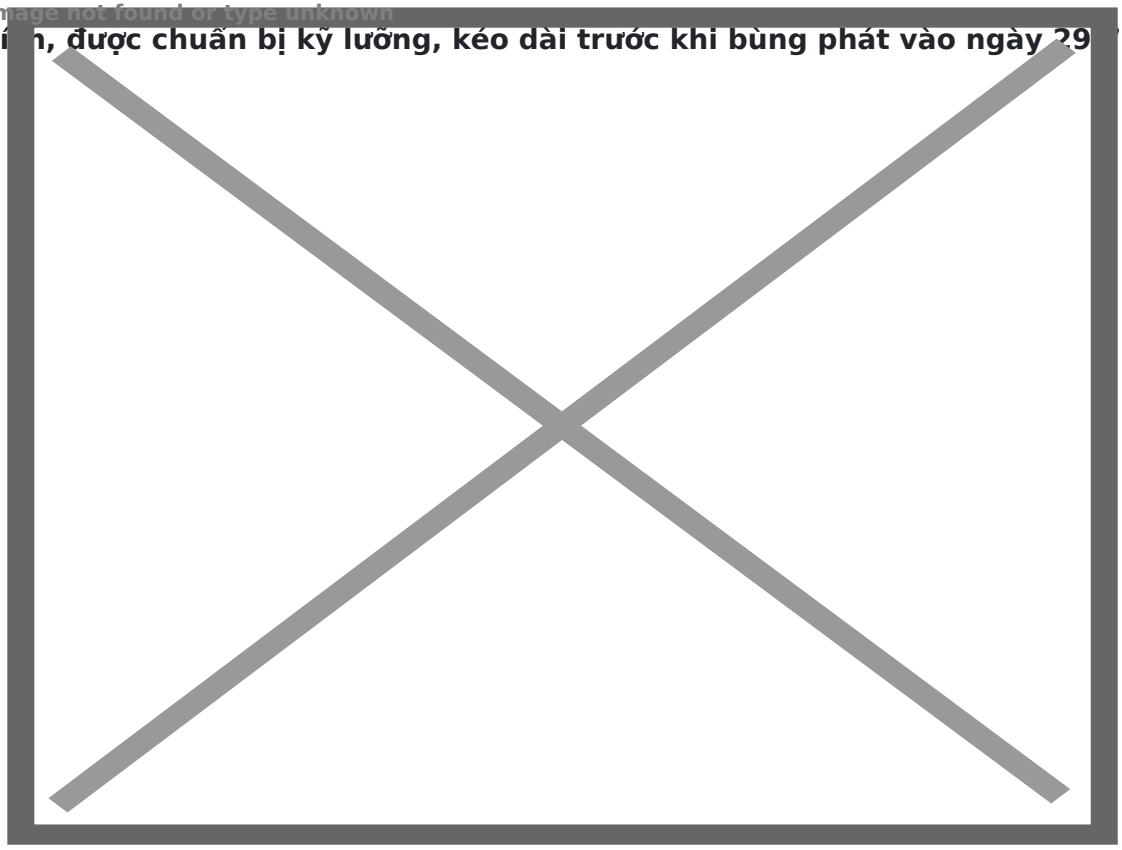
Hệ thống Vietnam Airlines có thể bị xâm nhập từ 2014

16:18 02/08/2016

Tác giả: Phạm Thùy Dung

Cuộc tấn công vào hệ thống của hãng Hàng không Quốc gia là dạng tấn công có chủ đích, được chuẩn bị kỹ lưỡng, kéo dài trước khi bùng phát vào ngày 29/7.



Màn hình hiển thị thông tin sân bay ở Nội Bài chiều 29/7 đã bị tắt sau khi bị tin tặc tấn công, chèn thông tin xấu

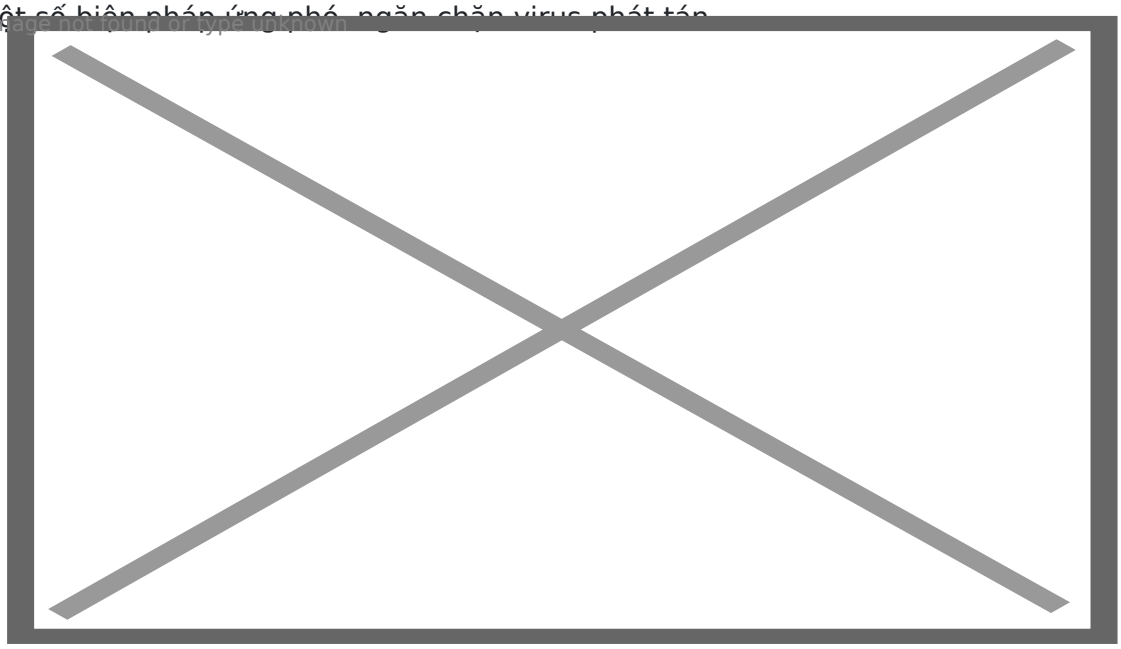
Theo Hiệp hội An toàn thông tin Việt Nam (VNISA), có dấu hiệu cho thấy có thể hệ thống đã bị tin tặc xâm nhập từ giữa năm 2014. Tuy nhiên, mã độc sử dụng trong đợt vừa rồi hoàn toàn mới, được thiết kế riêng cho cuộc tấn công ngày 29/7 và đã vượt qua được các công cụ giám sát an ninh thông thường, chẳng hạn các phần mềm chống virus.

Theo VNISA, những dấu vết để lại hiện trường chưa đủ cơ sở để kết luận chính xác đối tượng tấn công là ai. Song có thể khẳng định chúng am hiểu hệ thống công nghệ thông tin của các cụm cảng hàng không, cả ở mức cấu trúc thông tin lẫn cơ chế vận hành thiết bị. Đáng chú ý, chúng có ý định khống chế, vô hiệu hóa hoàn toàn dữ liệu hệ thống.

Bước đầu, đội ngũ an ninh mạng từ nhiều đơn vị đã xác định được mã độc phá hoại hệ thống và thấy rằng cửa hậu đã bị khai thác khá lâu trước thời điểm phát động tấn công.

Trước đó, chuyên gia bảo mật độc lập Nguyễn Hồng Phúc đã nhận định, khi tấn công vào website của Vietnam Airlines, hacker đã chia sẻ ba liên kết dẫn đến tập tin chứa dữ liệu khách hàng. Tài khoản ở đây được tạo ngày 25/7/2016, bốn ngày trước khi xảy ra cuộc tấn công. Do đó, theo chuyên gia này, thông tin của hơn 400.000 thành viên Golden Lotus có thể đã bị tin tặc khai thác 4 ngày trước khi thực hiện hack vào trang web của hãng Hàng không Việt Nam.

Về phía Vietnam Airlines, khi đánh giá về đợt tấn công của tin tặc ngày 29/7, ông Nguyễn Hải Tùng, Trưởng ban Công nghệ thông tin của hãng đã cho hay, các đối tác công nghệ thông tin của Vietnam Airlines đã phát hiện dấu hiệu nghi ngờ tin tặc xâm nhập từ tối 28/7 và đưa ra cảnh báo đợt virus này có khả năng bùng nổ trên diện rộng. Hãng Hàng không Quốc gia ngay sau đó đã có một số biện pháp ứng phó, ngăn chặn virus phát tán.



Khách xếp hàng trước quầy làm thủ tục lên máy bay khi hệ thống thông tin bị tấn công.

Khoảng 16h ngày 29/7, tại sân bay Nội Bài, Tân Sơn Nhất, nhiều hành khách đang làm thủ tục hốt hoảng khi thấy các màn hình thông tin chuyến bay bất ngờ thay đổi. Trên màn hình hiển thị các thông tin kích động, xúc phạm Việt Nam và Philippines, xuyên tạc các nội dung về Biển Đông. Hệ thống phát thanh của sân bay cũng phát đi những thông điệp tương tự. Sau khoảng 4 phút, nhà chức trách sân bay đã tắt toàn bộ hệ thống âm thanh, màn hình.

Cùng thời điểm, trên website của hãng hàng không Việt Nam cũng bị thay đổi nội dung, đồng thời đăng tải thông tin của hơn 400.000 thành viên Golden Lotus. Người dùng khi truy cập vào địa chỉ https://www.vietnamairlines.com, nhận được thông báo website đã bị hack, nội dung trang chủ được thay đổi hoàn toàn với các ngôn ngữ kích động.

Hôm nay, sau 3 ngày xảy ra sự việc, Vietnam Airlines thông báo hệ thống công nghệ thông tin chính của họ đã hoàn tất quá trình kiểm tra và trở lại hoạt động. Hãng đã phối hợp với các chuyên gia của Cục An ninh mạng (Bộ Công an), Cục an toàn thông tin, Trung tâm ứng cứu khẩn cấp máy tính Việt Nam VNCERT, Viettel, FPT và các đối tác khác để giành quyền kiểm soát, khôi phục và khởi động lại các chương trình bị tấn công cũng như rà soát chương trình khác để đảm bảo an toàn. Hãng bay đã phối hợp với Tổng công ty Cảng hàng không Việt Nam khôi phục các máy tính tại quầy làm thủ tục ở Nội Bài, Tân Sơn Nhất.

Đối với khách hàng chương trình Bông Sen Vàng, Vietnam Airlines thông báo sẽ tạm ngừng các chức năng trực tuyến, tuy nhiên vẫn đảm bảo đầy đủ quyền lợi của hội viên./.

Nguồn: VNE

Link bài viết: https://nguoilambao.vn/he-thong-vietnam-airlines-co-the-bi-xam-nhap-tu-2014