Nhiều cơ quan, doanh nghiệp ‘dính’ mã độc từng tấn công Vietnam Airlines

21:18 09/08/2016

Tác giả: Ngọc Bích

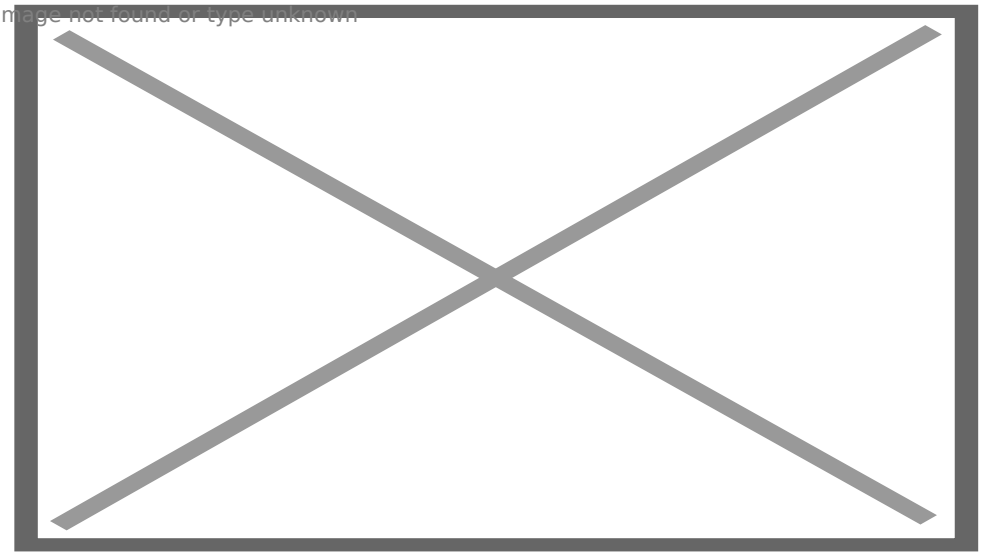
Ngày 8/8/2016, Tập đoàn công nghệ Bkav công bố kết quả phân tích cho thấy mã độc tấn công Vietnam Airlines cũng xuất hiện tại nhiều cơ quan, doanh nghiệp khác.

Ông Ngô Tuấn Anh, Phó Chủ tịch phụ trách An ninh mạng của Bkav, cho biết: “Bkav đã theo dõi mạng lưới phần mềm gián điệp tấn công có chủ đích (APT) vào hệ thống mạng Việt Nam từ giữa năm 2012. Kết quả phân tích cho thấy mã độc tấn công Vietnam Airlines cũng xuất hiện tại nhiều cơ quan, doanh nghiệp khác bao gồm cả các cơ quan Chính phủ, các tập đoàn, ngân hàng, viện nghiên cứu, trường đại học. Vấn đề này đã được Bkav nhiều lần cảnh báo rộng rãi”.

Trước đó, chiều ngày 29/07 website của Vietnam Airlines bị deface với hình ảnh nhóm hacker 1937cn, đồng thời dữ liệu của hơn 400.000 khách hàng Bông Sen Vàng bị rò rỉ lên mạng. Chưa dừng lại, hệ thống âm thanh và thông báo tại cảng hàng không Tân Sơn Nhất và Nội Bài bị can thiệp, sửa đổi hiển thị hình ảnh và âm thanh xuyên tạc về vấn đề Biển Đông. Ngay trong đêm 29/07, trong một bài phân tích trên WhiteHat.vn, các chuyên gia Bkav nhận định, để thực hiện được cuộc tấn công này hacker đã xâm nhập được sâu vào hệ thống bằng cách sử dụng phần mềm gián điệp (spyware) theo dõi, kiểm soát máy của quản trị viên.

Theo kết quả phân tích từ Bộ phận nghiên cứu mã độc của Bkav, mã độc sau khi xâm nhập vào máy tính sẽ ẩn mình dưới vỏ bọc giả mạo là một phần mềm diệt virus. Nhờ đó, nó có thể ẩn mình trong thời gian dài mà không bị phát hiện.

Image not found or type unknown



Sơ đồ mô tả phương thức tấn công của mã độc.

Mã độc có kết nối thường xuyên, gửi các dữ liệu về máy chủ điều khiển (C&C Server) thông qua tên miền Name.dcsvn.org (nhái tên miền của website Đảng Cộng sản). Trong đó Name là tên được sinh ra theo đặc trưng của cơ quan, doanh nghiệp mà mã độc nhắm tới.

Mã độc có chức năng thu thập tài khoản mật khẩu, nhận lệnh cho phép hacker kiểm soát, điều khiển máy tính nạn nhân từ xa, thực hiện các hành vi phá hoại như xóa dấu vết, thay đổi âm thanh, hiển thị hình ảnh, mã hóa dữ liệu… Ngoài ra, mã độc còn có thành phần chuyên để thao tác, xử lý với cơ sở dữ liệu SQL.

Hiện tại, Bkav đã phát hành công cụ quét và kiểm tra mã độc miễn phí, người sử dụng có thể tải công cụ kiểm tra tại link: Bkav.com.vn/ScanSpyware. Công cụ này không cần cài đặt mà có thể khởi chạy luôn để quét. Riêng người sử dụng Bkav Pro hoặc Bkav Endpoint sẽ được tự động cập nhật mẫu nhận diện mã độc này. Khi phát hiện hệ thống có mã độc, quản trị viên cần lập tức báo cho các cơ quan chức năng để được hỗ trợ rà soát toàn bộ hệ thống mạng vì khi mã độc này đã xuất hiện có nghĩa là hệ thống đã bị xâm nhập.

Nguồn: Infonet

Link bài viết: https://nguoilambao.vn/public/index.php/ma-doc-tan-cong-vietnam-airlines