Logo Logo not found or type unknown

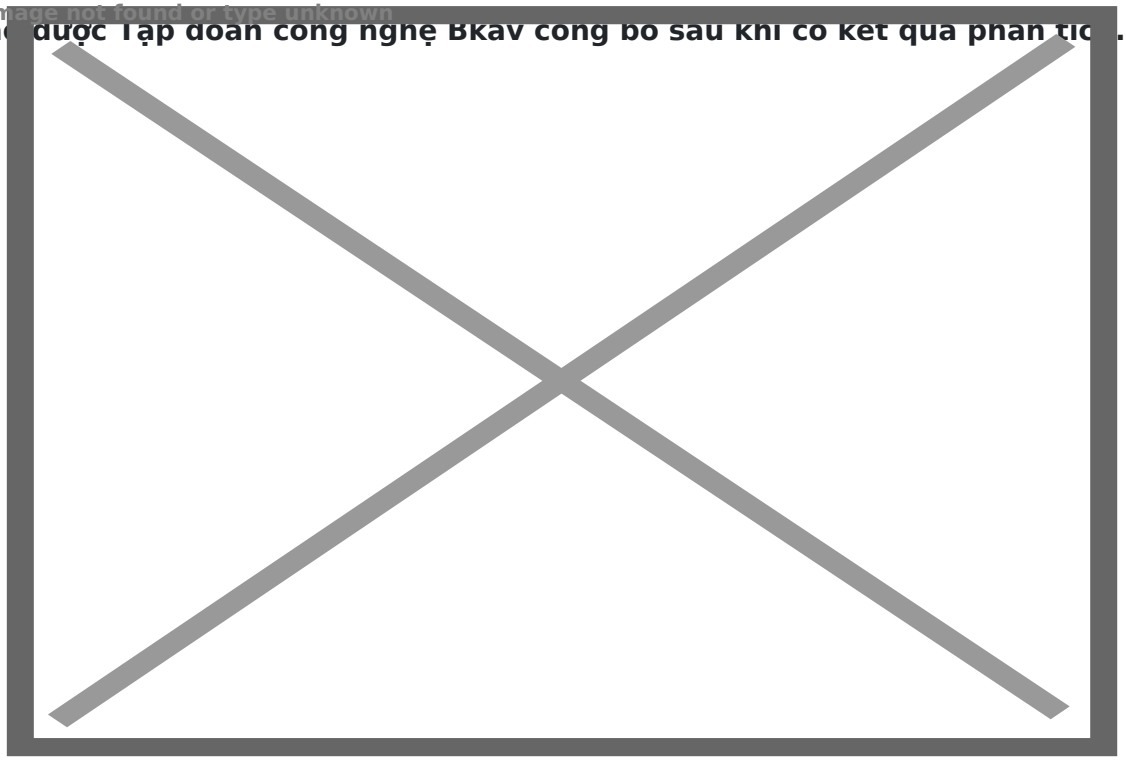
Mã độc tấn công Vietnam Airline hiện hình

22:22 08/08/2016

Tác giả: Phạm Thùy Dung

Mã độc tấn công Vietnam Airlines cũng xuất hiện tại nhiều trang web khác, đó là cảnh báo được Tập đoàn công nghệ Bkav công bố sau khi có kết quả phân tích.

Image not found or type unknown



Ảnh minh hoạ.

Nguồn: Internet

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.

“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”- các chuyên gia của Bkav cho biết.

“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” - chuyên gia Bkav nói.

Ông Ngô Tuấn Anh, Phó chủ tịch phụ trách An ninh mạng của Bkav cho biết: “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...”.

Bkav cũng cho biết, 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.

Trước đó, Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) cũng đã phát đi cảnh báo yêu cầu các cơ quan, tổ chức, doanh nghiệp... đặc biệt chú trọng công tác đảm bảo an toàn thông tin trên hệ thống do mình quản lý và quyết liệt thực hiện khẩn cấp một số biện pháp nhằm phòng tránh các cuộc tấn công có thể xảy ra.

VNCERT cũng yêu cầu các đơn vị này cập nhật thường xuyên các bản vá cho hệ điều hành, phần mềm dịch vụ trên các máy chủ, máy trạm, rà soát mã độc trên các máy chủ, máy trạm để phát hiện và gỡ bỏ sớm các mã độc đã được cài cắm.

Trong trường hợp phát hiện hệ thống CNTT có dấu hiệu bị tấn công, theo VNCERT, cần thực hiện một số bước cơ bản như sau: Ghi nhận và cung cấp các hiện tượng, dấu hiệu ban đầu cho đơn vị chuyên trách xử lý sự cố an ninh thông tin, nhanh chóng cách ly hệ thống có dấu hiệu bị tấn công, đồng thời giữ nguyên hiện trường hệ thống đang bị nhiễm, tạm thời sử dụng hệ thống máy chủ dự phòng cho các hệ thống chính, tiến hành thay đổi mật khẩu toàn hệ thống, đặc biệt là các hệ thống quan trọng như domain, cơ sở dữ liệu, ứng dụng core...

Đồng thời cần liên lạc ngay với đơn vị chuyên trách xử lý sự cố ANTT như VNCERT, Cục An ninh mạng - Bộ Công an.../.

Nguồn: TTO

Link bài viết: https://nguoilambao.vn/ma-doc-tan-cong-vietnam-airline-hien-hinh