BỘ CÔNG AN
CÔNG AN TỈNH SÓC TRĂNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 70 /TB-CAT

Sóc Trăng, ngày 07 tháng 10 năm 2022

THÔNG BÁO
Biến chủng mới của mã độc mã hóa dữ liệu

Thời gian gần đây, trên cả nước nói chung và tỉnh Sóc Trăng nói riêng xuất hiện tình trạng lây lan của dạng mã độc có tên **STOP/DJVU Ransomeware** *(hay còn gọi là **BESUB ransomeware**)*. Mặc dù **STOP/DJVU** không mới nhưng những biến thể của dạng mã độc tống tiền này ngày càng nhiều, vô hình chung gây khó khăn lớn trong việc ngăn ngừa, xử lý; một trong những dạng mã độc phổ biến nhất hiện nay là mã độc **QQJJ**.

Mã độc **QQJJ** *(một dạng biến thể của loại mã độc **STOP/DJVU** nguy hiểm)* được phân loại nhóm mã độc tống tiền. Sau khi xâm nhập vào máy tính, mã độc này bắt đầu thực hiện các chức năng cơ bản của một loại mã độc tống tiền. Đầu tiên, chúng sẽ quét các tập tin hệ thống và tất cả các dữ liệu được lưu trên máy tính, sau đó tiến hành mã hóa các tập tin đã quét được và thêm vào phần mở rộng **.qqjj** vào mỗi tên tập tin *(ví dụ: **1.jpg** sẽ trở thành **1.jpg.qqjj**)*. Sau khi bị mã hóa, nạn nhân sẽ không thể truy cập được vào các tệp này nữa, ngoài ra chúng còn để lại 01 tập tin có tên **_readme.txt** vào các thư mục có dữ liệu bị mã hóa để đòi tiền chuộc. Trong tập tin này có nội dung thông báo với nạn nhân rằng mã độc đã mã hóa toàn bộ dữ liệu cá nhân được lưu trữ trên máy tính và sẽ không thể khôi phục được nếu không có công cụ giải mã của đối tượng phát tán, ngoài ra chúng còn để lại một mức giá cụ thể và địa chỉ ví điện tử ảo để giao dịch. Mục đích của mã độc là tống tiền nạn nhân, chúng yêu cầu nạn nhân trả một khoản tiền để được khôi phục lại dữ liệu đã bị mã hóa. Tuy nhiên, không phải trường hợp nào chuyển tiền đều lấy lại được dữ liệu và thông tin cá nhân của mình.

Cũng như các phần mềm độc hại khác, loại mã độc này xâm nhập vào máy tính thông qua những tác vụ sau: Sử dụng phần mềm bẻ khóa (crack) có chứa mã độc; truy cập vào những trang web đen, đồi trụy; truy cập vào những trang web giả mạo, không an toàn; tải và cài đặt các phần mềm không rõ nguồn gốc, những ứng dụng lạ; mở tập tin (file) đính kèm có chứa mã độc trong email; nhấp vào các đường liên kết được đính kèm trong thư điện tử, một số loại quảng cáo giả mạo…

Loại mã độc tống tiền này rất nguy hiểm, khi dữ liệu đã bị mã hóa, khả năng phục hồi dữ liệu rất thấp, hiện chưa có công cụ nào có thể giải mã được nếu như không có khóa giải mã đặc biệt của đối tượng. Ngoài ra loại mã độc tống tiền này thường đi kèm với một số loại mã độc khác như mã độc **VIDAR**, **AZORULT**, những loại mã độc này có thể đánh cắp thông tin cá nhân như mật khẩu, lịch sử duyệt web, cookie, thông tin ngân hàng được lưu trên trình duyệt...

Trước diễn biến phức tạp của tình hình trên, nhằm phòng ngừa có hiệu quả đối với mã độc này, Công an tỉnh khuyến cáo:

(1) Thực hiện nghiêm chế độ bảo mật đối với các thiết bị lưu trữ bí mật nhà nước *(không cắm các thiết bị ngoại vi vào thiết bị khi chưa được sự cho phép, không kết nối internet đối với các thiết bị lưu trữ bí mật nhà nước...)*.

(2) Thường xuyên sao lưu các dữ liệu quan trọng *(trường hợp không may máy tính bị tấn công, đã có sẵn bản sao lưu dự phòng)*.

(3) Cảnh giác đối với các tập tin tải xuống: Đây là phương thức khá phổ biến của tin tặc, với việc gửi các tập tin với tiêu đề hấp dẫn qua thư điện tử hoặc qua các ứng dụng mạng xã hội nhằm dẫn dụ người dùng tải về. Khi tải về các tập tin này thường ở dạng ".docx", ".xlxs", ".pptx" hay ".pdf" nhưng thực chất đó là dạng tập tin thực thi ".exe" *(khi mở tập tin, mã độc sẽ bắt đầu hoạt động và tấn công vào máy tính người dùng)*. Để hạn chế nguy cơ bị mã độc tấn công, người dùng nên kiểm tra độ tin cậy của địa chỉ người gửi; thay vì mở tập tin trực tiếp (click trực tiếp lên tập tin), hãy sử dụng các phần mềm tương ứng như Word, Excel, Powerpoint... để mở tập tin (mở gián tiếp) vì nếu gặp tập tin thực thi (.exe), phần mềm sẽ báo lỗi.

(4) Hạn chế sử dụng các phần mềm bẻ khóa, không truy cập vào các quảng cáo, đường link nghi ngờ; máy tính phải được cài đặt phần mềm diệt virus có bản quyền, luôn theo dõi cập nhật dữ liệu virus mới nhất để chủ động trong việc bảo vệ thiết bị, bảo vệ dữ liệu; đảm bảo hệ điều hành và các phần mềm đang được sử dụng luôn được cập nhật thường xuyên, nhất là đối với các bản vá bảo mật.

(5) Nâng cao ý thức cảnh giác, cũng như trang bị những kiến thức cơ bản trong việc sử dụng các thiết bị công nghệ, các dịch vụ tiện ích, mạng xã hội, các dịch vụ thư điện tử để liên hệ công việc.

Công an tỉnh *(Thường trực Tiểu ban An toàn, An ninh mạng của tỉnh)* thông báo các đồng chí nắm phục vụ công tác phòng ngừa./.

Nơi nhận:
- TT.TU, UBND tỉnh (để báo cáo);
- Đ/c Giám đốc (để báo cáo);
- Các đ/c Phó Giám đốc (để nắm);
- Công an các đơn vị, địa phương;
- Các sở, ban, ngành, đoàn thể tỉnh;
- UBND các huyện, thị xã, thành phố;
- Lưu: VT, PV01 (TMAN), PA03.ĐTC(82b).

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
CÔNG AN TỈNH SÓC TRĂNG

Đại tá Huỳnh Hoài Hận