BỘ CÔNG AN **CÔNG AN TỈNH ĐẮK NÔNG**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 493/CAT-PA05 V/v cảnh báo tình trạng lây lan mã độc tống tiền Ransomware	*Đắk Nông, ngày 24 tháng 3 năm 2023*

Kính gửi:
- Các Sở, ban, ngành tỉnh Đắk Nông;
- Ủy ban nhân dân các huyện, thành phố.

Qua công tác bảo đảm an ninh, an toàn thông tin, Công an tỉnh phát hiện tình trạng lây lan mã độc mã hóa dữ liệu để tống tiền Ransomware diễn ra phức tạp với nhiều biến thể khác nhau gây hậu quả nghiêm trọng. Việc lây lan mã độc này chủ yếu qua tệp tin đính kèm email giả mạo, cài đặt các phần mềm không rõ nguồn gốc, sử dụng các thiết bị ngoại vi USB, ổ cứng di động và các vật mang tin khác sao chép dữ liệu từ các máy tính kết nối mạng internet với mạng nội bộ... Trước tình hình trên, Công an tỉnh thông báo đến các đơn vị các thông tin về hoạt động của mã độc và cảnh báo nguy cơ mất an ninh, an toàn thông tin như sau:

Mã độc Ransomware là phần mềm độc hại sử dụng thuật toán mã hóa bất đối xứng với khóa công khai "Public-key" và khóa bí mật "Private-key" để mã hóa dữ liệu người dùng. Khi dữ liệu bị mã hóa thì chỉ có khóa bí mật từ các đối tượng tin tặc *(đối tượng tạo ra mã độc Ramsomware)* mới có thể giải mã được. Ngay khi mã độc lây nhiễm vào máy tính sẽ thực hiện dò quét và tự động mã hóa, đổi tên các tệp tin tài liệu, dữ liệu, một số biến thể mã độc thuộc dòng này còn tiến hành khóa quyền sử dụng máy tính của người dùng. Sau khi mã hóa dữ liệu mã độc sẽ đưa ra thông báo yêu cầu người bị hại thanh toán tiền *(qua các tiền ảo bitcoin, Darkweb)* để lấy khóa bí mật giải mã các tệp tin mà mã độc đã mã hóa. Thời gian và giá trị tiền "chuộc" được mã độc đưa ra cho người dùng tùy thuộc vào loại biến thể của mã độc đang lây nhiễm trên máy tính người dùng. Đặc biệt, nghiêm trọng hơn dòng mã độc này còn chuyển hướng sang tấn công vào hệ thống máy chủ và mã hóa toàn bộ dữ liệu dẫn đến mất hoàn toàn dữ liệu và không thể khôi phục được. Các máy tính bị nhiễm mã độc thường có các biểu hiện như: các tệp văn bản được mã hóa đổi tên phần đuôi thành *.docm, *do.ccc, !RecoOveR, *.Cerber… và không thực hiện được bất kỳ thao tác nào trên các tệp này; máy tính trạm, máy tính chủ bị khóa màn hình *(Locker Ransomware hoặc Non-encrypting Ransomware)* và xuất hiện thông báo yêu cầu tiền "Chuộc"… Hiện nay, chưa có phần mềm hoặc dịch vụ ứng cứu sự cố

máy tính nào cho phép giải mã, khôi phục dữ liệu bị mã độc mã hóa nếu không có mã khóa của tin tặc phát tán mã độc.

Mã độc Ramsomware lây lan chủ yếu qua các phương thức như sau:

- Các đối tượng tin tặc giả mạo thư điện tử gửi các tập tin đính kèm chứa mã độc. Khi người dùng tải, kích hoạt tệp tin đính kèm này mã độc sẽ lây nhiễm vào máy tính.

- Các đối tượng đăng, chia sẻ các phần mềm miễn phí đã được bẻ khóa (không có bản quyền) có chứa mã độc lên các website, sau khi người dùng tải cài đặt phần mềm này mã độc sẽ lây nhiễm vào máy tính.

- Ngoài ra, máy tính còn có thể lây nhiễm mã độc thông qua việc kết nối mạng nội bộ, qua các thiết bị ngoại vi như USB, ổ cứng di động và các vật mang tin khác khi sao chép dữ liệu giữa các máy tính.

Trước tình hình trên, để tăng cường công tác đảm bảo an ninh mạng, an toàn thông tin, phòng ngừa mã độc Ramsomware trong tình hình hiện nay, Công an tỉnh Đắk Nông khuyến cáo các đơn vị thực hiện một số biện pháp như sau:

1. Quán triệt cán bộ công nhân viên chấp hành nghiêm quy định về bảo vệ bí mật Nhà nước, quy định về bảo đảm an toàn thông tin; thường xuyên tự kiểm tra, đánh giá việc tuân thủ các quy định bảo đảm an ninh, an toàn thông tin.

2. Chú ý cảnh giác với các tệp tin đính kèm, các đường dẫn được gửi đến qua thư điện tử hoặc tin nhắn, hạn chế tối đa việc truy cập vào các đường dẫn này. Tăng cường công tác quản lý việc sử dụng máy tính, thiết bị ngoại vi, thiết bị tin học trong Hệ thống quản lý, vận hành của đơn vị.

3. Triển khai biện pháp, giải pháp phòng chống mã độc; kiểm soát chặt chẽ việc cài đặt các phần mềm vào Hệ thống thông tin; sử dụng các phần mềm diệt virus kiểm tra các tệp tin gửi qua thư điện tử, tệp tin được tải từ internet trước khi mở, kích hoạt các tệp tin này.

4. Khi phát hiện máy tính bị nhiễm mã độc phải tiến hành cách ly ngay máy tính bị nhiễm ra khỏi hệ thống thông tin, mạng máy tính nội bộ, tuyệt đối không sử dụng các thiết bị mang tin như USB, ổ đĩa cứng di động…giữa máy bị nhiễm và các máy tính khác để tránh tình trạng lây lan. Có báo cáo kịp thời khi có tình trạng lây nhiễm mã độc, chủ trì phối hợp các đơn vị chức năng để khắc phục ứng cứu sự cố.

5. Thực hiện nghiêm túc việc sao lưu và bảo quản dữ liệu thường xuyên đúng quy định; tăng cường công tác quản lý và đề nghị các đơn vị có kết nối, chia sẻ dữ liệu thực hiện nghiêm các cam kết về đảm bảo an ninh, an toàn và bảo mật thông tin.

Công an tỉnh thông báo đến các đơn vị biết phòng tránh mã độc nêu trên./.

Nơi nhận:
- Như trên;
- Đ/c Giám đốc (để báo cáo);
- Lưu: VT, PA05 (Đ3), 35b.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Đại tá Hồ Quang Thắng